Examining Threats & Exploring Countermeasures

Selected Writings From
Protective Research Group

Protective Research Group

Table of Contents

Introduction ....

Fundamental Concepts of Terrorism 4
by Wade M. Knapp, CPS

Characteristics of Biological Warfare Agents 15
by Lee A. Knapp, RN, CEN

Understanding the Toxic Effects of Chemical Warfare Agents.......................... 25
by Lee A. Knapp, RN, CEN

Fundamentals of Encryption 36
by Nick LaFleur

Computer Viruses and Solutions 38
by Nick LaFleur

Understanding the Impact of Biological & Chemical Terrorism 41
by Wade M. Knapp, CPS

Using Passwords in a Computing Environment 44
by Nick LaFleur

Telephoned Bomb Threat Procedures 46
by Wade M. Knapp

Recognizing Letter and Package Bombs 48
by Wade M. Knapp, CPS

Understanding Crime Risk Management 53
by Wade M. Knapp, CPS

Security Patrol Operations 57
by Wade M. Knapp, CPS

Security Patrol Vehicle Maintenance 63
by Nick LaFleur

Safety at Automated Bank Teller Machines (ATM's).................................... 70
by Wade M. Knapp, CPS

Safety Precautions While Staying at Hotels or Motels..................................... 71
by Wade M. Knapp, CPS

Protection Officers and the Press 73
by Wade M. Knapp, CPS

First Aid Basics 75
by Lee A. Knapp, RN, CEN

Cyber-Cons On The Prowl 84
by Nick LaFleur

Leaving Children Home Alone 86
by Nick LaFleur

Internet Safety Tips for Children 88
by Nick LaFleur

Awareness Conditioning for Personal Safety 91
by Nick LaFleur

Chatting Terms and Abbreviations 93
by Nick LaFleur

Fundamentals of Vehicle Safety 96
by Wade M. Knapp, CPS

Biographical Profiling for Personal Safety 99
by Wade M. Knapp, CPS

Copyright Bibliography 101

About the Authors 103

Introduction

Today's global political and social landscape is a canvas of rapid change . The continued and increasing threat of Terrorism and Crime confront us on a daily basis in the United States. The risks of Bombings, Chemical & Biological Terrorism, Cyber-Terrorism, Workplace Violence, School Violence, and Traditional Crime have become commonplace in our society. The facts regarding these threats have been confirmed by U.S. Government Agencies, Research Organizations, as well as the global news media. And it appears that these threats will follow us well into the next decade, and beyond. The effective management of these threats will require knowledge, skill, and training not only on the part of our emergency response community, but the general public as well. Only by working together can we protect our society and its citizens today and into the future.

Protective Research Group is a consulting firm located in Jacksonville, Florida that provides consulting and training services in issues relating to personal, corporate, and public protection and safety. We utilize an aggressive approach to consulting and research projects with the goal of providing our clients with cutting edge, no-nonsense results, which can then be applied in the real world. Our members are some of the most professional and experienced instructors in the fields of safety and protection. Dedicated to providing a high-energy learning experience through informative, thought provoking training seminars which encourage participant interaction. Our core consulting and training areas include: Terrorism Awareness, Chemical & Biological Terrorism, Bomb Threat Management, Personal Protection, Executive Protection, Computer Security, Information Profiling, First Aid and CPR Training.

This book contains a series of 23 articles authored by the members of Protective Research Group. The subject matter of these articles span a wide range of protection issues including terrorism, computer security, bomb security, protection officer training, and personal safety. The purpose of this book is to introduce the reader to our group and the issues in which we provide consultation. This book is also meant to act as a tool to enhance your current safety program by providing a no-nonsense insight into real world threats and threat countermeasures.

Fundamental Concepts of Terrorism

by

Wade M. Knapp, CPS

It is often said that "One man's terrorist is another man's freedom fighter." This statement illustrates the common diversity of the term terrorism. One person's opinion of what terrorism is may, differ from that of another person. So then, what is "terrorism" and how do we define it? The answer to this question depends upon an individual's own perspective of terrorism and how it affects them. The same is true for governments that battle with the threat of terrorist violence on a daily basis.

Webster's Dictionary defines "**terrorism**" as; "the systematic use of terror especially as a means of coercion," and "**terror**" is defined as; "a state of intense fear": "one that inspires fear": "a frightening aspect": "a cause of anxiety": "violence committed by groups in order to intimidate a population or government into granting their demands." This is a general definition of terrorism which can be applied to a wide range of situations, from the school yard bully to an airplane hijacker.

The military definition of terrorism is the one that most accurately fits the traditional model of political terrorism. Terrorism in itself is nothing but a tactic of a larger division of warfare known as "psychological warfare." Psychological warfare operations are composed of strategies designed to assist conventional military tactics in the defeat of an opposing force through psychological means. These tactics are meant to harass, intimidate, instill fear, unbalance, coerce, etc. these opposing forces. Tactics can include propaganda or disinformation operations, sabotage, assassination, kidnaping, bombings, threats of violence, etc. The use of terrorist tactics such as these have been employed by military forces since the beginning of warfare itself. The military concept of terrorism is usually the foundation for the political definition of terrorism used by most governments.

The political definition of terrorism is generally the one that is accepted as the legal standard for the term. This is due to the fact that terrorism must be defined in such a way that the legislation of laws regarding the concept can be created. And even though the political definition is generally the one which becomes the standard, there is not a single global definition of terrorism that can be agreed upon. Different governments, as well as agencies within governments, may define terrorism in similar terms but also in slightly different ways. This too is usually based upon the perspective of the individual government or agency. The United States Government, for example, defines the term "Federal crime of terrorism" as "an offense that is calculated to influence or affect the conduct of government by intimidation or coercion, or to retaliate against government conduct," the term is also defined in further detail regarding the nature of offenses. The Federal Bureau of Investigation defines "terrorism" as "the unlawful use of force or violence against persons or property to intimidate or coerce a government, civilian population, or any segment thereof, in furtherance of political or social objectives." Both of these definitions have the same basic meaning, they are just worded differently because they are applied in different ways.

In the United States, the Federal Bureau of Investigation's definition of terrorism is generally the one most commonly used by Law Enforcement agencies, as well as the general public. This is not to say that the FBI's definition of terrorism is the absolute, but it does define the concept in a simple and concise manner which makes it a very functional definition. It tells us that terrorism is the use of violence against persons or property in the name of political or social objectives. It is important to understand the distinction between the use of violence motivated by political or social reasons, and the use of violence for other reasons. The use of terrorist type violence alone does not qualify as terrorism. A disgruntled ex-employee who bombs his former employer's building in revenge for being terminated has committed a crime, not an act of terrorism. Violence must be motivated by the furtherance of a political or social agenda before it can be considered an act of terrorism. This political or social element is all important when defining what is, and isn't terrorism. True terrorism is violence perpetrated, by individuals or groups, with the goal of bringing about political or social change within a government or population. All violence committed which lacks this political or social element will be considered "crime."

Terrorism Classifications

- **International & Domestic Terrorism**

Terrorism can be divided into two basic categories; international terrorism and domestic terrorism. Fundamentally, both of these types of terrorism are the same when it comes to the threat they present, tactics and weapons used, motivations, group structures, etc. The difference between international and domestic terrorism is found in geographical location.

International terrorism refers to terrorism that is perpetrated against American interest by groups or individuals that are citizens of a foreign country. These terrorist groups or individuals, along with their motivations and ideologies, will originate and reside abroad. These terrorists generally view America as the enemy and whether they attack an American target in a foreign nation or here in the United States, it will still be classified as an act of international terrorism. International terrorism can include classifications such as; State Directed Terrorism, State Sponsored Terrorism, Narco Terrorism, Single Issue Terrorism, and Religious Terrorism.

Domestic terrorism refers to terrorism that is perpetrated against American interests by Americans. These types of terrorist groups and individuals, along with their motivations and ideologies, originate and reside in the United States. And whether they attack an American target here in the United States or abroad in a foreign country, it will still be classified as domestic terrorism. Domestic terrorism can include classifications such as: Left Wing Terrorism, Right Wing Terrorism, Narco Terrorism, Single Issue Terrorism, and Religious Terrorism.

- **State Directed Terrorism**

State directed terrorism refers to acts of terrorism against American interests perpetrated by groups or individuals operating as agents of a foreign government. This type of terrorism is generally conducted by nations which consider The United States an enemy. These groups or individuals will have received training, support, funding, and operate under the direct control of that government. Such groups or individuals will generally be associated with official military or security forces of the foreign government. The motivations for the use of terrorism by a foreign nation could include retaliation for military action, or political and economic sanctions used against that country.

- **State Sponsored Terrorism**

Terrorist groups or individuals which receive support from a host nation in the form of training, equipment, funding, and a base of operations, are known for being state sponsored. Terrorist groups or individuals in this category operate independently, and not under the control of the host nation. The terrorist group will have no official connection to the host country, but may operate for the country covertly in return for the support provided. Nations which support terrorism may do so for many different groups of varying ideologies simultaneously. The groups themselves may also be receiving support from other nations as well. In return for this support, these groups would be available to conduct terrorist operations for multiple nations, at the same time advancing their individual group agenda or movement.

- **Single Issue Terrorism**

Single issue terrorism, also known as ‘special interest terrorism’, is a type of terrorism in which a group or individual commits acts of terrorism in the name of one specific cause or movement. This type of terrorism is most commonly seen associated with causes or movements such as abortion, animal rights, environmental issues, etc. Generally, these groups are solely committed to their causes and don’t form alliances with groups representing other social or political causes. Acts of terrorism are generally directed toward corporate or government entities which are viewed as in opposition to the group’s movement. These types of terrorist groups or individuals can originate internationally or domestically.

- **Narco Terrorism**

Narco terrorism is violence perpetrated by drug trafficking cartels and organizations. This type of terrorism is primarily directed toward government entities which conduct interdiction operations against the drug organization or toward other drug trafficking organization viewed as competition. These types of terrorist groups or individuals can originate internationally or domestically.

- **Right Wing Terrorism**

Right Wing Terrorism refers to terrorist groups or individuals, who’s ideology and movements are generally anti-government in nature. The focus of this type of terrorism can be single or multi-issue in nature, and can include issues such as anti-taxation, pro-constitutional rights, anti-law enforcement, anti-federal government, etc. These types of groups have been known to form alliances with other groups with similar, or even opposing, ideologies. Groups that are associated with Right Wing movements include; Nazi groups, Hate groups, Anti-tax groups, Militias, etc. Groups with these ideologies can be found operating both internationally and domestically.

- **Left Wing Terrorism**

Left Wing Terrorism refers to terrorist groups or individuals, who’s ideology and movements are generally concerned with social issues. The focus of this type of terrorism is generally single issue in nature, and can include issues such as; anti-abortion, pro-animal rights, pro-environmental, anti-technology, etc. These types of groups may form alliances with other left-wing groups with similar, or even opposing, ideologies. These groups may also be international or domestic.

- **Religious Terrorism**

Religious terrorism is violence perpetrated in the name of some religious doctrine or belief. This type of terrorism can be found associated with groups or individuals from both established mainstream religions, as well as “fringe” religious movements. “Fringe” religions are generally associated with “cults,” while other groups are found to be rooted in mainstream Western, Eastern and Middle Eastern religions. Basic examples of this type of terrorism can be found in incidents of violence associated with the anti-abortion movement in the United States, or with Middle Eastern groups who have declared "Jihad"(Holy War) against the United States. Groups or individuals associated with this type of terrorism are found to be very dedicated to their movements and believe they are being directed by the word of God in most cases. This type of terrorism can be both International or Domestic in nature.

- **Individuals**

Acts of terrorism do not necessarily have to be perpetrated by a group. A lone individual terrorist can pose the same level of threat as an entire group. Some consider the threat of terrorism posed by individuals to be greater in some respects than that of groups. This is due to the fact that the movements of individuals are much more difficult to track than that of groups. The individual can harbor and develop his terrorist agenda and planning in total seclusion without the need of outside assistance. We probably will not know of this individual's existence until after a terrorist act has been committed. Individuals engaged in terrorism could range from the professional terrorist who makes his living working for terrorist groups or nations, to the average person living in the average community. Either way, it makes this type of terrorism a very dangerous prospect for any government or civilian population.

The Tactics and Weapons of Terrorism

The tactics of terrorism are easy to define and include; political assassination, kidnaping, hostage taking, direct armed assaults, armed facility occupations, hijacking of aviation and ground transportation, bombings, industrial sabotage, propaganda and disinformation campaigns, threats of violence, etc. In general, these tactics are meant to destroy, kill, injure, intimidate, coerce, disrupt and unbalance the established enemy and ultimately force that enemy into political or social change.

Any weapon has the potential for use by a terrorist group, but some weapons are used more often than others. Bombs are used in the vast majority of terrorist incidents, making the bomb the number one weapon of choice. Statistics point to bombs being used in more than 80% of all terrorist incidents. Bombs are used more frequently than any other weapon for several reasons. Bombs are relatively easy and inexpensive to make, easy to conceal and transport, they can be built to suit specific needs, cause extensive amounts of damage to property, injure large numbers of people at one time, and inflict great fear or psychological terror on the community.

Firearms are the second most widely used weapons of terrorism. Firearms and ammunition are available globally through civilian, military or black market sources. Firearms are easily concealed and transportable, require only minimum skill to operate, and are capable of creating extensive damage both physically and psychologically. We all understand the terror associated with images of a man in a mask carrying an assault weapon.

In addition to bombs and firearms, attention recently has begun to focus on what is known as Weapons of Mass Destruction (WMD). Weapons of Mass Destruction are specifically designed to result in the death or injury to large numbers of people at one time. These Weapons of Mass Destruction fall into four basic categories: Nuclear Weapons, Biological Weapons, Chemical Weapons, and Large Conventional or Improvised Bombs.

Nuclear Weapons pose the greatest threat of potential death and destruction, but their potential for use by terrorists is limited due to several factors. Nuclear weapons, and the raw materials used to make these weapons, are strictly controlled on a global wide basis. They are extremely difficult and expensive to make or acquire, and easily detectable by governments using sophisticated radiological monitoring devices.

Biological weapons pose as great a threat as do nuclear weapons, and their potential for use by terrorist groups is thought to be feasible. Biological weapons incorporate the use of diseases such as Anthrax, Smallpox, Plague, or any other number of biological organisms as weapons. The biological organisms utilized as weapons are available in nature and require only minimal scientific knowledge to produce them as weapons.

Chemical weapons also pose a high threat for potential use by terrorist groups, but pose less of a threat of damaging effects than do Nuclear or Biological weapons. This is due to the nature of chemical compounds in general. While chemical weapons may have a quicker and more devastating initial effect when used, they don't have the wide spread effect of a biological weapon because they are not communicable agents. There are no "outbreaks" associated with the use of chemical agents, but they can be very lethal and cause extensive contamination at the site of usage. Chemical weapons also do not possess the shear destructive power of a nuclear weapon. The real threat associated with chemical weapons is in the fact that chemicals are available in every community in the United States, making their use as a potential weapon extremely high.

The last category of Weapons of Mass Destruction is large explosive devices. These bombs may be conventional military devices such as missiles and aerial bombs, or improvise devices such as large vehicle or truck bombs. Their potential for use by terrorist groups is extremely high, due to the fact that they have already been used on several occasions in the recent past. Examples of the use of such devices can be found in the incidents involving the Murrah Federal Building in Oklahoma, the World Trade Center in New York, and the bombings of two American Embassies in Africa. These types of devices are easy to manufacture, with the necessary components being widely available globally.

The Structure of A Terrorist Group

In the traditional model of a terrorist group, we see that the organizational structure is similar to that of any business. There is a leadership element, an active operational element, support elements, etc. all working together for the common goal of the group. Generally, the size of the group's membership base will increase and widen from the top, downward. You can expect to see more active operational members than leaders, and more support members than active members, etc.

- **The Leadership Section**

The task of leadership in the terrorist group will generally be similar to that of the leadership of any other organization. The leadership section of the terrorist group would be responsible for the overall management of the group, developing group philosophies and goals, operational planning, group development, providing direction for the members, etc. Terrorist leaders are generally highly intelligent and motivated, well educated, possess good leadership qualities, are charismatic, etc. They would also be responsible for obtaining and maintaining financial and political support for the group.

- **Intelligence Support Section**

Members of the intelligence section of the terrorist group would be tasked with information gathering responsibilities. These members would conduct surveillance activities against possible targets, conduct information research to assist planning and operational elements of the group, etc. Surveillance methods utilized by terrorist groups could include, wiretapping, physical surveillance, computer system intrusion, open source information research, Internet research, video and photographic surveillance, etc. Information may also be obtained through paid informants working for the group. The extent and sophistication of the group's intelligence gathering apparatus is only limited by the group's imagination and resources.

- **Active Support Section**

Active support members could be tasked with any number of group functions. In smaller terrorist groups, the active membership element could be responsible for the bulk of the group's activities. These members could be responsible for creating and distributing group propaganda, acquiring and maintaining group safe-houses, logistical support, transportation, intelligence gathering, executing operational aspects, member recruitment, etc. Generally, the active support element of a terrorist group would contain the most members as compared to other elements of the group. This section could include members from a wide variety of occupations and backgrounds, depending upon the skills and resources needed by the group. Active members could include various skilled laborers, mechanics, medical or scientific personnel, merchants or businessmen, individuals with military experience, etc.

- **Tactical Support Section**

Members of the tactical section would be responsible for conducting the active operational requirements of the group. These members would conduct the actual terrorist acts, which could include bombings, hijacking, kidnaping, assassinations, etc. These members would have received training in the use of weaponry, military style tactics, bomb making, etc. They may have backgrounds in traditional military services, have a firm dedication to the group's goals, and capable of using violence to achieve those goals. Tactical support members may also be responsible for providing security for the group and providing training to other members. Depending upon the size and resources of the group, tactical support members could either be paid professionals hired by the group, or dedicated followers of the group's movement, or a combination of both.

- **Passive Support Element**

Generally, passive support members are those individuals which provide support to the group's movement, but don't participate in active or violent operational functions. These members may support the group in the form of conducting protest or marches to raise public awareness of the group's movement, provide logistical support, contribute financially to the group, etc. A cross section of the general population may be represented in this section and could include family and friends of active members.

Beyond this general organizational structure, any individual terrorist group could take on its own unique structure depending upon its size and resources. For example, a smaller terrorist group containing only 25 members may be divided into a leadership and operational section only. Due to the small size of the group, there would be no need for several sections tasked with different duties, the operational section would simply provide these functions. In addition, a large terrorist group may divide itself even further into what is referred to as "cells."

These cells are smaller sections of the parent group operating independently, but under the direction of the parent group. Cell groups can operate as a smaller version of the parent group, maintaining the same organizational structure, or operate under a narrow chain of command. The size and structure of the cell would greatly depend upon the nature of the cell's operational responsibility. For example, a large terrorist group based in a Middle Eastern country may deploy and maintain a smaller branch of the group in a European country. The smaller cell group located in the European country may be structured and responsible for the same operational goals as the parent group. The cell would contain a leadership, active and passive support elements, tactical elements, etc., except on a smaller scale. A cell could also be composed of members from a single operational element of the parent group tasked with a specific function. The cell may be solely responsible for intelligence gathering, propaganda publishing and distribution, carrying out terrorist attacks, etc. Due to the small nature of cell groups, the parent terrorist organization could deploy several cells to different geographical locations simultaneously. These cells' groups may even operate without knowledge of each other, making them more difficult to track.

Who Is a Potential Target of Terrorism?

The answer to the question 'Who is a potential target of terrorism?' is an easy one. Any individual, corporation, organization, government, nation or civilian population located on the globe is a potential target for terrorism. No one is absolutely immune from this type of violence, the very nature of terrorism assures that truth. At one time or another, entities from every sector of our society, as well as the global community, have fallen prey to the violence of terrorism. Buildings are bombed, planes hijacked, government and corporate officials are kidnaped or assassinated, nations threatened, soldiers and citizens murdered, etc. Incidents such as these have occurred and will continue to occur, as long as groups or individuals choose to utilize terrorism as a method of airing their grievances. The problem exists in the fact that we can't accurately predict when and where the next act of terrorism will occur, or what the nature of the act will be. This reality is the underlying reason for the effectiveness of terrorism as a psychological, as well as physical, weapon. Even if you are not the victim of a direct act of terrorism, you're affected collaterally by the fear, anxiety, distrust, and uncertainty that an act of terrorism creates. And while it may be true that in general anyone can fall victim to an act of terrorism, certain types of targets present themselves as tactically more attractive than others. These include such targets as:

- Federal, State or Local government facilities
- Political or corporate officials
- Military facilities
- Public transportation systems
- Corporate and industrial facilities
- Public events
- Historic landmarks
- Educational facilities
- Public utilities
- Nuclear energy facilities
- Computer systems and networks
- Food or water supplies
- Consumer products
- Agriculture and livestock

Terrorist Target Selection

How do terrorists select their targets? The answer to this question is a little more complex then one might think. On the surface it would appear that incidents of terrorism occur randomly, as if out of the clear blue. News reports often refer to terrorism as random acts of senseless violence which, for the most part, occur for little or no reason. In reality, nothing could be further from the truth. Yes, while the victims of a terrorist act may be random, the act itself was not.

A terrorist is, in much the same way, similar to a common criminal. Criminal acts are also not random in nature. A criminal must possess the desire, the ability, and the opportunity to commit a crime. Desire, ability and opportunity are therefore known as the elements of the crime, and their presence establishes some degree of pre-planning. Just as the criminal will conduct planning prior to committing a burglary, robbery, murder, car-jacking, theft, or any other number of crimes, the terrorist will plan a bombing, hijacking, assassination, etc. This process of planning removes the element of randomness in the act. What appears random to the average citizen is actually thought out in advance. Where randomness does play a part is in the fact that several terrorist incidents may have nothing in common with each other. The acts may have occurred at different times and places, may have employed different tactics, or were perpetrated by different groups for completely different motivations.

To better understand how terrorists select potential targets, we will examine several key elements of the process. First we will assume the terrorist or a terror group possesses the desire to commit an act of terrorism. Desire, which could also be called motivation, is the psychological element in the overall process. It is the underlying reason for the act. The intended target may or may not know the motivation for the attack prior to it happening. The terrorist may issue public statements or threats regarding his motivations prior to an attack, or wait until after the attack when responsibility is claimed. The terrorist may also never communicate the motivation for the attack, leaving us to wonder why? The motivations which fuel the terrorists act are many and can be simple in nature, or very complex. Motivations for committing terrorist acts include:

- The furthering of political, social or religious agendas
- Bringing public awareness to the group's cause or movement
- Creating panic, fear and distrust among a target population
- Destruction of industrial capabilities
- Revenge
- Morale building within the group or movement
- Financial gain
- Assisting with the defeat of an opposing military force

In addition to desire, we will also assume the terrorist or a terror group has the ability to commit such acts. Ability is the physical element in the process and includes all the necessary skills, knowledge, equipment and resources needed to carry out the attack. Lastly we have opportunity, the element which creates the need for a target. Because without a target to attack, desire and ability alone would accomplish nothing for the terrorist or terror group.

It is in the process of searching for the right opportunity to commit the act of terrorism that target selection becomes so important. Selecting the right target will require the terrorist or terror group to conduct research and planning. The criteria used by terrorists to select their targets is composed of several elements. If the target fits the operational elements of this selection criteria, it may be chosen for attack. The selection criteria is as follows:

- **Accessibility.** To successfully attack the target, the terrorist must penetrate the target's defenses. Does the target allow easy access to the terrorist?

- **Vulnerability.** Even if the terrorist gains access to the target, is the target vulnerable to attack? Targets are generally categorized as either "soft targets" or "hard targets." A soft target is one in which the potential target employs lower levels of security measures. This type of target is considered easily vulnerable to the terrorist's attack. A hard target is one in which the potential target employs higher levels of security measures, making it more difficult to attack.

- **Criticality.** How critical is the target in terms of the terrorist's object? Will an attack on the target benefit the terror group, or result in obtaining the specific goals of the group?

- **Suitability.** Is the target suitable to the group's political or operational objectives? Whom has the group declared as the enemy? Does this target represent the established enemy?

- **Recuperability.** How quickly can the target recuperate from the attack? The goal will be to disrupt the target's operation for as long as possible.

- **Effect on the group.** Will an attack on the target create the intended effect for the terror organization? Will this effect on the group be positive in the eyes of its supporters?

- **Risk.** What is the risk to the operational element conducting the attack? Can the terrorists escape after the attack? What is the risk of confronting police or government agents?

The degree to which each of the elements of the above criteria are applied will greatly depend upon the terrorist group's operational requirements. For example, if the terrorist group's plan calls for the suicide bombing of a target, then the risk posed to the attacker is of less importance than accessibility. In general, it would be valid to assume that if a potential target fits the above criteria the terrorist group may consider it viable for attack.

Characteristics Of Biological Warfare Agents

by

Lee A. Knapp, RN, CEN

Background On Biological Warfare Agents

Biological warfare is the use of microorganisms (bacteria, viruses, and fungi) or toxins (poisons from living organisms) to produce death or disease in humans, animals, and plants. Biological agents are the oldest of the nuclear, biological, chemical (NBC) triad and have been used by governments in warfare for 2,500 years. These agents are more deadly on a compound per weight basis than chemical agents. Biologic agents occur naturally in the environment, but many have been refined and could be made more resistant in laboratories.

During the 1991 Persian Gulf War, the threat of biological warfare against American soldiers increased the public awareness of the possibility of a potential biological attack against U.S. cities. The reality of this threat gained credence in 1996 when two high ranking Iraqi military officials revealed that during the war, Iraq had produced and prepared to use 19,000 liters of botulinum toxin and 8,500 liters of anthrax.

Rogue nations and terrorist organizations have shown a strong interest in the use of biological weapons (BW) because these weapons are inexpensive to produce, difficult to monitor, and can produce illness and death in large numbers of people. Called “the poor man’s nuclear bomb,” biological weapons can be produced with minimal startup equipment and supplies and can be introduced easily into areas with large groups of people. Fifteen to twenty-five countries are thought to possess biological weapons. Five countries supporting terrorism may have biological weapons. These agents are appealing to countries with limited resources.

- **Characteristics**

Biological agents may be found in the form of bulk or compacted powders, gels, or liquids. Their intended effects, determined by the terrorist group, can be incapacitating or lethal and may be communicable or noncommunicable. Biological warfare agents have the potential for causing widespread illness and death.

Bacteria are single-celled microorganisms that vary in shape depending on the makeup of their cell wall. Cocci are 0.5 to 1 micron is size. Bacilli are 1 to 5 microns in size. Bacteria are self-sustaining organisms that do not require a host to reproduce. Some types, such as anthrax, may transform into a spore and remain alive in a dormant state.

Viruses are the simplest type of microorganism and are composed of only genetic material (RNA or DNA) surrounded by a protein coat. Viruses are much smaller that bacteria and require a host to function and survive. This host can be plant, animal, insect, bacteria, or human. Many viruses attack a specific type of cell causing disease or cancer.

Biological toxins are nonliving, poisonous chemical compounds that are produced by living organisms (animals, plants, and microorganisms). Biological toxins produce illness and disease by a variety of mechanisms, including interfering with nerve conduction, interacting with the immune system, and inhibiting protein synthesis. Toxins are more toxic per weight than manmade chemical agents, but unlike chemicals, toxins are not typically volatile or able to cause illness through skin absorption. Person-to-person transmission does not occur and toxins are not very persistent when released. The toxicity of these agents varies by the route of entry into the body.

The primary route of infection for biological weapon agents is by inhalation, although other routes such as ingestion, dermal abrasion, and intentional percutaneous routes have proven effective. Since biological weapon agents are nonvolatile (do not evaporate), they must be dispersed in aerosols as 1 to 5 micron size particles (1/30,000 of the diameter of a hair follicle). At this size, particles deposit deep into the terminal air sacs of the lungs, causing disease. Smaller particles do not remain in the lungs and larger particles are too large to reach the lungs.

ANTHRAX

Bacillus anthracis is a gram-positive, rod-shaped organism that reverts into a resistant spore under adverse environmental conditions. These spores may be viable and infectious for up to 50 years. Once a spore enters a host, it becomes infectious by germinating into a macrophage. It is then transported to regional lymph nodes where local production of toxins cause edema and death of tissues. Bacteremia, toxemia, and death will follow. Anthrax is an endemic infection in animals, particularly sheep. Humans may naturally become infected if handling contaminated animal fluids or hides, this disease is known as "Woolsorters Disease".

Anthrax causes disease after inoculation of open or minor skin wounds, ingestion, or inhalation of the spores. The inhalation route has the highest mortality rate and is most likely to be used by terrorists, in it's wet or dry powder forms, because of it's easy dissemination from a spraying device. Untreated skin infections which develop into septicemia have a 20 % mortality rate, 1 % for treated infections. The mortality rate greatly increases to 80 to 90 % mortality rate when anthrax involves the lungs (inhalation) or intestines (ingestion).

Anthrax spores were weaponized by the United States in the 1950's and 1960's before the old U.S. offensive program was terminated. Other countries have been or are suspected of weaponizing this agent.

Cutaneous Anthrax

Skin lesions appear 1 to 5 days after spores have been introduced into open skin. Vesicles ranging from 1 to 2 cm in size appear with regional edema and lymphadenitis occurring. Most patients with small lesions may present afebrile. The lesions develop into a painless necrotic ulcer with a black eschar base. The ulcer may spontaneously heal within 2 to 3 weeks, however, 20 % of these cases may develop septicemia and death. Following a major intentional attack, it is possible that cutaneous anthrax cases might appear in conjunction with inhalational cases.

Gastrointestinal Anthrax

Symptoms of gastrointestinal anthrax are variable, but might include fever, nausea, vomiting, abdominal pain, bloody diarrhea, and sometimes a rapidly developing ascites. These patients may present with an acute abdomen. Oropharyngeal cases show primary involvement of the tonsils.

Inhalational Anthrax

Following the inhalation of a small amount of anthrax spores, alveolar macrophages engulf the spores and the bacteria become vegetative. After transportation to the tracheobronchial nodes, a 1 to 6 day incubation period begins. This incubation period is followed by early non-specific symptoms of fever, malaise, myalgias, nonproductive cough, and/or chest discomfort. These symptoms seem to improve over a few days returning with a sudden onset of respiratory distress, dyspnea, and stridor. The chest x-ray may reveal a hilar or mediastinal adenopathy or widened mediastinum with or without a bloody pleural effusion. Typically the chest x-ray does not show evidence of infiltrates. Once toxins elaborate, medications are ineffective. Septicemia, toxic shock, and death usually occurs in 24 to 36 hours.

PLAGUE

Yersinia pestis is a gram-negative, rod-shaped organism that is non-motile and does not sporulate. The organism is killed easily when exposed to disinfectants, sunlight and temperatures above 72° C for 15 minutes, but is resistant to near freezing temperatures and can remain viable in dry sputum, flea feces, and buried bodies. Plague, also known as the cause of "Black Death" of 14th Century Europe which killed over 25 million people, is normally a disease of rodents, but can be spread to humans by fleas living on infected rodents (rats, mice, ground squirrels). Prairie dogs in the southwest U.S. are major reservoirs of plague. It has been shown that domestic dogs exhibit a resistance to this infection, but domestic cats are highly susceptible. Transmissibility in man is high and all humans are susceptible to the disease. Effects are usually lethal with a 30 to 100% mortality rate. If recovery from the disease occurs, it may be followed by a temporary immunity. Since 1993 there have been 15 confirmed cases of plague in the United States. Nearly all fatal plague cases in the U.S. result from delay in seeking treatment or from improper diagnosis.

Plague produces disease by being consumed by macrophages and is then transported to regional lymph nodes causing regional adenitis. Entry into the blood stream causes infection in secondary organs such as the lungs, spleen, liver, and brain. Infection occurs in three forms: **bubonic,** which involves the lymph nodes closest to the bite of infected fleas (usually lower legs); **pneumonic,** which is an infection of the lungs from inhalation; and **septicemia,** which is a generalized infection in the blood from the bacteria escaping through the lymph nodes or lungs causing toxic shock. Dissemination can occur naturally from the bites of fleas, or used as a terrorist's weapon and disseminated via aerosol (inhalation) or introduced into food/drink (ingestion).

Bubonic Plague

Bubonic plague occurs from the bite of an infected flea. Initial symptoms include erythema, fever, and chills which typically progresses to bubo formation in regional lymph nodes. Septicemia normally develops 2 to 10 days later. Buboes may be aspirated but should not be surgically drained. Gram staining is diagnostic. Bubonic plague may progress spontaneously to the septicemic form involving multi system organs, and may also cause vasculitis, resulting in purpura and thrombis from stimulating the clotting cascade resulting in gangrene. Bubonic plague is not usually transmitted person to person unless there is contact with pus from draining buboes. Universal precautions and contact isolation should be employed when treating these patients.

Pneumonic Plague

After inhaling the organism, either through aerosolization as a biological weapon or from respiratory droplets from another infected person, a 2 to 3 day incubation period occurs followed by a sudden onset of high fever, chills, and flu-like symptoms. Within 24 hours, fulminant pneumonia and systemic toxicity are seen. Chest x-ray may show patchy infiltrates or consolidation. Coagulation abnormalities are common and severe ecchymosis may occur ("black death"). Bloody sputum will produce positive cultures for yersinia pestis. This pneumonia progresses rapidly, causing dyspnea, stridor, respiratory failure, and circulatory collapse. Six percent of pneumonia cases have an accompanying meningitis. Acral gangrene may be a late complication of pneumonic or septicemia plague, and occur in the fingers, toes, earlobes, nose, and penis.

TULAREMIA

Francisella tularensis is a non-motile, gram-negative cocco-bacillus that typically causes disease in animals (rabbit fever, deer fly fever). Humans become infected with the disease by handling contaminated animal fluids or through bites by deer flies, mosquitoes, or ticks. Tularemia does not form spores, but the organism can remain viable for weeks in many environments. It is resistant to freezing but is sensitive to heat and disinfectants. After infection occurs, bacteria spread to regional lymph nodes and reticuloendothelial system. Bacteremia with secondary spread to the lungs and other organs follows. Almost all of those exposed to tularemia will become infected. The mortality rate for persons who go untreated is 20 - 30%, with a mortality rate of 5% for treated victims. Recovery is followed by permanent immunity.

Infection occurs via inhalation, ingestion, or absorption. Inhalation is the most deadly route of exposure. Inhaling as few as 10 to 50 organisms will cause disease, whereas millions of organisms must be ingested to produce disease. Ingestion or inoculation, through minor skin lesions or arthropod bites, results in the ulceroglandular form of tularemia. With its easy spread ability, tularemia may be an effective weapon for terrorists.

- **Symptoms**

Within 2 to 10 days after inhalational exposure, patients develop abrupt onset of high fever, chills, headache, myalgias, non-productive cough, and pneumonia. If the organism was ingested or inoculated, symptoms will also include regional lymphadenopathy and may or may not have cutaneous ulcers. Pronounced inflammation and necrosis may occur in the lymph nodes, lungs, skin, conjunctiva, or oropharnyx. Long term complications may include hepatitis and renal damage.

Q FEVER - RICKETTSIAL TYPE

"Query" fever, or Q fever, is caused by Coxiella burnetii which is a highly infectious rickettsia microorganism resistant to heat and drying. A rickettsia is an obligate parasitic bacterium that requires a host to survive, similar to a virus. C. brunetii becomes engulfed by a phagocyte where it multiplies and disseminates to multiple organs and reticuloendothelial system. Initially, this organism causes the host cell to increase its metabolic and functional activity, leading to eventual cell rupture. Q fever typically causes infection in animals such as sheep, cattle, and goats. This organism reactivates in female sheep during pregnancy, with up to a billion organisms found per gram of placenta. Humans can acquire the disease by inhaling aerosols contaminated with the organism. Inhaling only one organism can cause infection.

Q fever is considered probably the very best of the biologicals to be used as an incapacitating agent by terrorists. The primary forms can be wet or dry and can be disseminated by aerosol or as contaminated food/drinks. C. brunetii grows well in eggs, it lives long and hardy in air, and will hit the ground before it dies if dispersed by aerosol. Q fever is usually a self-limiting disease in non-immunocompromised individuals, even without treatment. Antibiotics only shorten the course of disease. The mortality rate is less than 1%.

- **Symptoms**

Ten to twenty days after inhalation, there is a sudden onset of an influenza like syndrome with marked anorexia. Symptoms can include fever, chills, blinding headache, general weakness, severe sweats, and chest pains. An atypical pneumonia is seen in 50% of the cases. X-ray may reveal a "ground glass" appearance. One-third of the patients may show elevated liver enzymes. Neck stiffness and CNS signs may also occur. Patients are not generally critically ill. The illness can last from 2 days to 28 days.

SMALLPOX

Variola virus, an Orthopox virus, caused both minor and major forms of the smallpox disease. Smallpox was declared eradicated in 1980 and the U.S. stopped its civilian vaccination in 1981. The U.S. military stopped its vaccination program in 1985. Supposedly, only the U.S. and Russia posses repositories of the virus, concerns over clandestine stockpiles of the agent still remain. The Soviet Union was thought to have weaponized the agent. In the recent past, we have seen human monkey pox epidemics occur in Zaire. It is possible that this agent could become available to terrorist groups for future use. The overall clinical course of monkeypox in humans is equivalent to that of smallpox, but is milder with a lower mortality rate.

Smallpox is a highly contagious agent that could be produced and disseminated easily as a biological weapon. The primary forms of smallpox can be wet or dry with an aerosol dissemination method. Mortality rates with natural borne exposure in the past were 20 to 40% in previously unvaccinated individuals and 3% in those who had received the vaccine.

Since the smallpox vaccine is no longer given, and the vaccine that has been given only gives immunity for 10 years, the American public could be at great risk should a terrorist attack using small pox take place.

- **Symptoms**

Ten to twelve days after airway exposure, influenza-like symptoms such as fever, mild erythematous rash, headache, severe backache and occasional abdominal pains occur. Within 2 to 3 days, exanthema on the face, arms, and hands is noted. Over a period of 8 to 10 days, initial macules become papules and typical pustular vesicules progressing to scabs. Patients remain contagious until all scabs are healed over. Differential diagnosis is make between varicella (chicken pox) with varicella causing crops of lesions that start primarily on the trunk and spreads to the extremities. Small pox lesions are syndronous in their development all over the body.

VENEZUELAN EQUINE ENCEPHALITIS (VEE)

Venezuelan Equine Encephalitis (VEE) virus is a mosquito-borne alphavirus usually infecting horses, mules, and donkeys. It is endemic in certain parts of the world - Central and South America, Mexico, and Florida. VEE is characterized by inflammation of the meninges of the brain and the brain itself, thus accounting for the predominance of Central Nervous System (CNS) symptoms of the small amount of infections that develop encephalitis. The disease is usually acute, prostrating, and of short duration. VEE is highly infectious with nearly 100% of exposed individuals developing symptoms. The mortality rate for natural borne infection (through mosquito bites) is about 1%. Recovery from this infection results in excellent short-term and long-term immunity.

VEE was weaponized by the United States in the 1950's and 1960's before the old U.S. offensive biowarfare program was terminated. Other countries have been or are suspected of weaponizing this agent as well. VEE could be produced in either a wet or dried form and delivered easily as an aerosol. The virus can be destroyed by heat (80° C for 30 minutes) and ordinary disinfectants. If this agent was released intentionally by terrorists, disease might occur simultaneously in both horses and humans. However, a terrorist use of VEE as an aerosol would be likely to have a considerably higher mortality rate considering the virus is trophic to the olfactory nerves and could gain access to the Central Nervous System via this route.

- **Symptoms**

In 1 to 5 days following exposure, symptoms of fever, chills, intense headache, photophobia, myalgias, nausea, vomiting, and diarrhea begin. These symptoms tend to last up to 3 days followed by a prolonged period of weakness and lethergy. Recovery is usually seen in 1 to 2 weeks. Only a small percentage of victims (20% of children, 4% of adults) will exhibit symptoms of meningitis and encephalitis. As mentioned above, if an intentional aerosolized attack occurred, a greater percentage of patients with CNS involvement may be seen. If patients develop CNS symptoms such as meningitis, seizures, change in mental status, or coma, the mortality rate increases to 20%, especially in children. Permanent neurological problems have been reported.

VIRAL HEMORRHAGIC FEVERS

Viral Hemorrhagic Fevers are a diverse group of illnesses caused by a variety of RNA viruses with a wide range of morbidity and mortality. The clinical syndrome which these viruses cause in humans is called VHF. VHF is caused by four RNA virus families: the Filoviruses, the Bunyaviridae, the Flaviridae, and the Arenaviridae. These viruses use a variety of insect or rodent vectors and include: Ebola, Marburg, Dengue, Yellow Fever, Crimean-Congo Fever, Hantaan Viruses, and Lassa Fever. Each of these viruses has a unique history and is capable of being spread to humans by aerosol or fomite, and by contact with blood and body fluids. Many of these fevers can be treated effectively except for Ebola. VHF agents, especially Marburg and Ebola have allegedly been considered for weaponization.

Ebola and Marburg, which are filoviruses, were made famous in the non-fiction book “The Hot Zone” and the fictional works of Executive Orders and Outbreak. Outbreaks of this virus have occurred in Sudan and Zaire in 1976, in Sudan in 1979, and in Zaire in 1995 where there were 300 cases. In the U.S., a related virus (Ebola Reston) was isolated from a group of laboratory monkeys imported from the Philippines in 1989.

Not all infected persons develop VHF. Reasons for this varies depending on various host factors, differences between virus strains, and other immunologic factors. However, a consistency remains between each of these

RNA viruses is that the target organ is the vascular bed. Widespread microvascular damage and changes in vascular permeability causes blood leakage from vessels.

- **Symptoms**

Patients with VHF present initially with fever, myalgias, and prostration. Clinical findings may include conjunctival injection, petechial hemorrhages, and hypotension. Full-blown cases will develop into shock with generalized mucous membrane hemorrhaging, involvement of respiratory, hematopoietic , and central nervous systems. Laboratory evaluation may reveal renal insufficiency, abnormal liver function studies, and elevated bilirubin levels. All of these findings reflect a poor prognosis. Mortality rates range between 50 and 80 % for Ebola strains.

BOTULISM

In 1994, CDC reported 34 cases of food borne botulism in the U.S. Most outbreaks result from eating improperly preserved home-canned foods, with vegetables canned in oil being the most common source.

Botulinum toxin is a neurotoxin produced by the bacteria, Clostridium botulinum, which causes the disease botulism. This toxin is the most lethal compound per weight and is approximately 15,000 times more toxic that the nerve agent VX. Botulinum toxins produce similar effects whether the agent is inhaled or ingested. The primary form of botulinum toxin for use by a terrorist would be in a powdered form and could be disseminated by aerosol (less likely), in consumables such as food and drink (most likely and most effective route), and via projectiles. However, the onset of symptoms varies between hours and days, depending on the route of exposure and the initial dose.

Botulinum works by irreversibly binding to the presynaptic neuromuscular junction and preventing the release of acetylcholine (ACh) there and at cholinergic autonomic sites. This interruption of neurotransmission causes both bulbar palsies and skeletal muscle weakness. A bulbar palsy is a cranial neuropathy that produces a loss of function in the nerves that originate from the brain stem. These conditions do not reverse until the nerves grow back in approximately 6 to 8 weeks.

- **Symptoms**

Within 12 to 36 hours after exposure to the toxin, a descending paralysis (head-to-toe) and bulbar palsies become the characteristic symptoms. Symptoms include blurred vision, mydriasis (dilated pupils), diplopia (double vision), ptosis (drooping eyelids), photophobia, dysarthria, and dysphagia. Soon after, skeletal muscles become weak, starting in the upper body and moving downwards in a symmetrical fashion. Progression of symptoms including respiratory failure will occur in as little as 24 hours. Patients usually remain awake and alert.

RICIN

Ricin is a potent cytotoxin that is derived from castor beans and is a by-product of castor oil production. Over a million tons of castor beans are used each year in the production of castor oil. When compared with VX, ricin is over 200 time more toxic by weight. Ricin is considered a potential biological weapon because of it’s worldwide availability. Some believe that ricin is a likely agent for assassinations.

Ricin can be prepared in liquid or crystalline form, or dried into a powder. It can be effectively disseminated by aerosol, introduced into food supplies, and can also be injected. Ricin is a very stable compound and is extremely toxic by either of these routes.

Ricin works by blocking protein synthesis within the cell. When inhaled, it causes necrosis of the airways.

- **Symptoms**

With inhalation of ricin, victims would begin to experience fever, chest tightness, cough, shortness of breath, nausea, and joint pain within 4 to 8 hours after exposure. Ricin causes airway necrosis and pulmonary edema. Death may occur in 36 to 72 hours.

If ricin was ingested, victims would develop rapid onset of nausea, vomiting, severe diarrhea, and gastrointestinal hemorrhage. Necrosis of the liver, spleen, and kidneys would occur. Vascular collapse would follow with death occurring in 3 days.

By injection, ricin causes marked death of muscles and lymph nodes near the site of injection. Multiple organ failure occurs leading to death.

STAPHYLOCOCCAL ENTEROTOXIN B (SEB)

SEB is a fever producing exotoxin produced and excreted by the bacteria Staphylococcus aureus. Illnesses related to this toxin usually occur after ingesting improperly handled foods that have an overgrowth of staph organisms. Inhalation of SEB does not occur naturally and symptoms will vary depending on the route of exposure. Once this toxin enters the body, it causes a large proliferation of T-cell lymphocytes and stimulates the production and secretion of various interleukins and cytokines. These events are thought to mediate the toxic effects seen with SEB.

SEB is an incapacitating type agent even at sublethal doses. Over 80 % of those exposed individuals will develop symptoms. Fatality rate is < 1%. It is most often seen as a dry powder and may be dispersed as an aerosol or introduced into the food supply.

- **Symptoms**

With ingestion of SEB, patients will present with symptoms of nausea, vomiting, and diarrhea which may be severe in nature.

With inhalation, sudden onset of high fever (103 to 104 F), chills, headache, generalized myalgias, and non-productive cough are expected to develop within 3 to 12 hours following exposure. Severe shortness of breath and chest pain will develop with larger doses. Chest x-ray will usually be non-specific, but in severe cases, pulmonary edema and ARDS may develop. Fever may last 2 to 5 days, and cough may persist up to 4 weeks.

TRICHOTHECENE MYCOTOXINS (T2)

The trichothecene mycotoxins are low molecular weight nonvolatile toxins produced by several species of filamentous fungi (molds). These toxins are naturally occurring, usually found in improperly stored grains that have become wet and infected with trichothecene producing molds. Trichothecene mycotoxins are stable for long periods of storage and are highly persistent. They are extremely stable to heat and ultraviolet light. These mycotoxins are fast acting potent inhibitors of protein and nucleic acid synthesis. Their main effects are to rapidly proliferate tissues, much like vesicants. Disease results if this toxin is inhaled, ingested, or has contact with skin. Of the various toxins produced, T2 is the most stable and therefore most likely to be used in a terrorist attack. The potential for use as a BW toxin was demonstrated to the Russian military shortly after World War II when flour contaminated with species of Fusarium was unknowingly baked into bread that was ingested by civilians. Some developed a protracted lethal illness called alimentary toxic aleukia (ATA). Mycotoxins allegedly have been used in aerosol form (“yellow rain”) to produce lethal and nonlethal casualties in Loas, Kampuchea, and Afghanistan.

- **Symptoms**

Within minutes of exposure, erythema of the skin accompanied by pain and a burning sensation occurs. Blisters form and progress to necrosis with leathery blackening and sloughing of large areas of skin in lethal cases. Eye pain, tearing, redness, foreign body sensation and blurred vision may follow entry of toxin into the eyes. Inhalational exposure produces a rapid onset of nasal itching and pain, sneezing, rhinorrhea, epistaxis, cough, dyspnea, wheezing, chest pain, and hemoptosis. Anorexia, nausea, vomiting, and watery or bloody diarrhea with abdominal cramping occurs with gastrointestinal toxicity. Systemic toxicity may follow by any route and is manifested by weakness, prostration, dizziness, ataxia, and loss of coordination. These toxins cause radiomimetic injury of intestines, bone marrow, lymph nodes, spleen, and thymus, resulting in leukopenia and bone marrow atrophy. Tachycardia, hypothermia, and hypotension follow in fatal cases. Death may occur in minutes, hours, or days.

Understanding The Toxic Effect Of Chemical Warfare Agents

by

Lee A. Knapp, RN, CEN

Background On Chemical Warfare Agents

Chemicals were first used as warfare agents during World War I. In 1915, Germany released 168 tons of chlorine onto troops at Ypres, Belgium. In 1917, sulfur mustard was used by German troops again at Ypres, Belgium. The first chlorine attack represented merely an escalation of the existing use of chemicals as irritants. The use of irritating smoke, such as the burning of sulfur, against opposing forces dates back to antiquity.

Various agents can be irritating, incapacitating, can injure or kill. Some agents cause only local effects, some have only systemic effects, while others have both effects. An irritating or incapacitating agent could cause a retreat or render persons unable to advance allowing a terrorist time to accomplish his or her goal.

Some chemicals may evaporate quickly while others may remain for long periods of time. This is described as their persistency. Persistence can be from minutes to days and is determined by the chemistry of the agent and the environment in which it is used.

Chemical agents can be in the form of solids, powders, liquids or gases. Agents may be inhaled, swallowed, or enter the body through eyes or skin. The effects can be immediate or delayed.

Twenty-five to thirty countries have active military programs. Since chemicals are readily available or easily made, of low cost, are easily transportable, and can be delivered by varying routes, chemicals make an excellent weapon for the terrorist. Most countries, including the United States, are not prepared to deal with a terrorist attack using chemicals.
The following information is designed to provide you with a basic knowledge of these chemical warfare agents and their toxic effects. In addition, basic information regarding the decontamination procedures and medical treatment of these chemical agents has also been included. This information is being presented with the goal of assisting the general public with developing a greater understanding of the chemical warfare agents which could be used against us by terrorist.

NERVE AGENTS

The nerve agents are **Tabun** (GA), **Sarin** (GB), **Soman** (GD), and **VX.** These are the most toxic of all the weaponized military agents. Nerve agents are classified as organophosphates which have physiological effects similar to that of many insecticides commonly found in the community. GB, or Sarin, is one of the more commonly stockpiled agents and the most publicly well known due to the Tokyo subway incident.

When dispersed, the more volatile ones constitute both a vapor and liquid threat. Sarin may be inhaled as a vapor, or cause toxic effects by contact with the skin in the liquid form. VX is primarily a liquid skin hazard at normal ambient temperatures. These chemicals are easily absorbed through the skin, eyes, or lungs and can cause sudden loss of consciousness, seizures, apnea and death. Onset of noticeable effects occur from a few seconds to hours after exposure. Nerve agents are designed to irritate, incapacitate, injure or kill.

- **Characteristics**

Nerve agents are stored and transported in the liquid state. The G-agents are volatile liquids at normal temperatures, although, the most volatile, Sarin, evaporates at about the same rate as water.

- **Toxicity and effects**

Nerves communicate with muscles, organs, and other nerves by releasing chemicals or neurotransmitters at their connection site (synapse). One of the most common neurotransmitters is acetylcholine (ACh), which is released and collects at the receptor site stimulating the end organ to respond and produce a variety of effects: muscle contractions, gland secretion, and nerve-to-nerve conduction.

When a nerve impulse reaches the synapse, acetylcholine is released from the nerve ending and diffuses across the synaptic junction to combine with receptor sites of the receiving nerve, and the electrical message continues. To stop further stimulation of the nerve, acetylcholine is rapidly broken down by acetylcholinesterase (AChE). Thus, a “check and balance” system prevents the accumulation of acetylcholine and the resultant over-stimulation of nerves, muscles and glands.

The term “nerve agent” refers to chemicals that produce biological effects by inhibiting the enzyme acetylcholinesterase, thus allowing the neurotransmitter acetylcholine to accumulate. As a result of this accumulation, the organ that is normally stimulated has now become over-stimulated which causes hyperactivity of this organ.

The clinical effects of nerve agents are in organs that have cholinergic receptors. These are divided into muscarinic sites (smooth muscles and exocrine glands) and nicotinic sites (skeletal muscles and pre-ganglionic fibers). Over-stimulation at muscarinic sites will increase secretions. The victim may experience increased saliva, tearing, runny nose, phlegm in the airways, and sweating. The accumulated acetylcholine also causes pinpoint pupils (miosis), shortness of breath (bronchoconstriction), and hyperactivity of the gastrointestinal tract (nausea, vomiting, and diarrhea). Over-stimulation of niocotinic receptors causes skeletal muscle fasciculation, twitching, cramping, weakness, and finally paralysis. There is also stimulation of the pre-ganglionic fibers which may contribute to hypertension and tachycardia.

Nerve agents can also have further effects on the cardiovascular system. Bradyarrhythmias, heart block, tachyarrhythmias (sinus tachycardia), and ventricular arrhythmias (ventricular tachycardia and ventricular fibrillation) may occur, but most disappear once the antidote is given.

The central nervous system may be effected in other ways as well. Acute severe effects include loss of consciousness, seizures, and apnea. Effects from a mild exposure include nervousness, fatigue, minor memory disturbances, irritability, and other minor psychological symptoms. These latter symptoms may be prolonged for 4 to 6 weeks following exposure to a nerve agent.

The diagnosis of a nerve agent poisoning must be made clinically. There usually is not time for laboratory confirmation. ***The combination of pinpoint pupils and muscle fasciculations is the most reliable clinical evidence of organophosphate (nerve agent) poisoning.***

VESICANTS

Vesicants cause blistering to the skin. There are many types of vesicant causing agents such as plants, animals, chemicals and sunlight. As for chemical warfare agents, sulfur mustard and Lewisite are the most commonly referred to. There is no medical pretreatment for blister agents. There is also no specific therapy, only supportive measures.

SULFUR MUSTARD

Sulfur mustard poses a threat in it's vapor and liquid forms. If inhaled, damage to the respiratory tract occurs which can lead to respiratory distress and possibly respiratory failure.

With contact to the eyes and skin, mustard can cause temporary blindness and blistering of the skin. Because of mustard's radio mimetic effects, damage to some internal organs can also occur.

If mustard has contact with the skin, it is absorbed and chemical cellular damage occurs within one to two minutes. There is no immediate pain, there is no immediate skin discoloration or blistering, and there is no immediate eye irritation. Hours later, the casualty realizes that he or she has been exposed. The onset time for clinical effects ranges from two to 48 hours with the most common time frame of four to eight hours.

The exact mechanism by which mustard damage's cell is not fully understood. It alkylates DNA and clings to proteins and other cellular components. The end result is DNA damage and cellular death. Because of such cellular destruction, more extensive injury can result in death because of sepsis as a result of bone marrow damage, decrease in white blood cells, and an impaired immune system.

- **Characteristics**

Mustard is an oily liquid with a color ranging from a light yellow to brown. It's odor is that of garlic, onion, or mustard, although odor should not be relied upon for detection.

- **Decontamination**

Decontamination must be done as quickly as possible since cellular damage occurs in as little as two minutes. Decontamination of the casualty at the ED 30 minutes or more after contact with mustard will not change the clinical course of the patient's illness, but will prevent cross-contamination of providers. The casualties should remove all clothing, rings, and jewelry. Skin decontamination may be performed with soap and water or with a 1:10 bleach solution and flushed well with water afterwards.

- **Eye injury and treatment**

Eye involvement can range from mild conjunctivitis from a small exposure of mustard, to more severe conjunctivitis, lid inflammation and edema, blepharospasm, and corneal roughening with a larger exposure. These more severe effects will cause the casualty to be unable to open their eyes and will render them without sight. A larger exposure, particularly if by liquid, may produce corneal opacification, corneal ulceration, or corneal perforation. Miosis is sometimes observed after mustard exposure and is thought to be due to cholinergic effects.

Gentle irrigation of eyes with saline or water should performed initially. Aggressive attempts to pry apart severely painful, blepharospastic eyelids to accomplish an irrigation 30 minutes or more after exposure is of little value, since the damage has been done and the agent has evaporated or has been absorbed. A visual acuity should be obtained prior to initiation of further treatment measures. With severe eye injuries, homatropine or other mydriatics should be applied topically to prevent adhesion formation. Topical analgesics may be used for the initial examination, but further use should be avoided. The instillation of topical steroids may be of benefit if used within the first 24 hours. Topical antibiotics should be applied several times per day and vasoline should be applied to lid edges to prevent them from adhering. Oral analgesics is the preferred route for pain management. The eyes should never be bandaged, although the wearing of sunglasses may be beneficial. Early involvement of an ophthalmologist is advised.

- **Skin injury and treatment**

Skin effects begin hours after exposure with erythema accompanied by burning and itching, followed later by the development of small vesicles. Later these small vesicles coalesce to form blisters. The size and depth of the blister formation depends on the amount of the exposure and whether the exposure was from vapor or liquid. Coagulation necrosis extending into the dermis may develop under blisters caused by the accumulation of liquid.

Soothing creams or lotions might be effective for irritation and burning. Oral pain medications will also be needed. Large blisters should be unroofed and these areas should be irrigated several times a day. Topical antibiotics should be applied to prevent skin bacterial superinfections. Fluid requirements should be addressed, although fluid replacement is much less than with thermal burns. Rarely will burns be full thickness requiring skin grafting.

- **Airway injury and management**

Mustard damages the mucosa or lining of the airways. This damage begins in the upper airways and descends downward into the lower respiratory tract depending upon the dose exposure. A relatively small exposure may cause upper airway irritation resulting in epistaxis, sore throat, and a hacking cough. A moderate exposure may cause hoarseness, laryngitis with voice loss and a productive cough. A larger exposure which reaches into the lower respiratory tract and effects the bronchioles may produce dyspnea and a productive cough. Because of damage that could occur to the underlying musculature as well, hemorrhagic pulmonary edema is possible, although pulmonary edema is rare.

Upper or minor airway symptoms may be relieved by steam inhalation and cough suppressants. A patient with moderate to severe effects may benefit from oxygen, bronchodilators, steroids, or continuous positive airway pressure (CPAP). For signs of severe upper airway involvement, intubation should be preformed early before laryngeal spasm or edema makes it difficult. The initial chemical pneumonitis should be treated in the usual manner, but antibiotic therapy should not be started until after an organism has been identified.

- **Gastrointestinal effects**

Initial gastrointestinal effects of nausea and vomiting usually occur within the first 24 hours following an exposure. These effects are due in part to the cholinergic stimulation. Some added effects may be from swallowed tracheal secretion. Gastrointestinal effects seen after 3 to 5 days are thought to be due to tissue destruction in the abdomen.

- **Bone marrow effects**

Absorption of significant amounts of mustard produces damage to and death of the stem or precursor cells of the bone marrow. This causes a decrease in white blood cells, red blood cells, and platelets 3 to 5 days following exposure. The absence of these cells increases susceptibility to infection. Survival is rare if WBC counts become less that 200.
Reverse isolation precautions should be initiated early for those patients who have had a large exposure to mustard.

LEWISITE

Lewisite is a vesicant that is rapidly absorbed by the eyes, skin, and lungs. It produces blisters similar to mustard, however, Lewisite is highly irritating on initial exposure. It also produces visible lesions more quickly. Unlike mustard, it does not damage bone marrow.

- **Characteristics**

Lewisite is an oily, colorless liquid with the odor of geraniums. It is more volatile than mustard.

- **Decontamination**

Decontamination must be done to remove contaminant prior to allowing entry into the ED to prevent cross-contamination to staff members. Careful removal of the casualties clothing, rings, and jewelry must be accomplished to prevent further exposure of the patient to the agent. Skin decontamination may be performed with soap and water or with a 1:10 beach solution and flushed well with water afterwards. Irrigation of eyes should be performed using saline solution or water in copious amounts.

- **Eye injury and treatment**

Lewisite causes pain and blepharospasm on contact. Edema of the conjunctiva and lids follows and the eyes may be swollen shut within an hour. Iritis and corneal damage may follow if the dose is high. Treatment protocol for eye injuries from mustard should be referred to when treating Lewisite exposures.

- **Skin injury and treatment**

Lewisite causes much greater skin damage than mustard. Skin irritation is seen relatively soon after exposure causing immediate pain or irritation. A gray area of dead skin is often seen prior to progression to blister formation, severe tissue necrosis and sloughing although the full lesion does not develop for 12 to 18 hours.

Treatments of such blistering tissue damage is the same as for mustard. Patients should be observed closely for signs and symptoms of infection occurring in wounds.

- **Airway injury and management**

Lewisite causes immediate irritation to the upper airways. Because of this extreme irritancy to the nasal area and upper airways, it causes the person to mask or exit the area quickly. The airway mucosa is the primary target and damage progresses down the airways in a dose-dependent manner. Further severe lung damage can occur if casualty is not removed from the area of contamination quickly. Pseudomembrane formation is commonly seen. Pulmonary edema, which is rarely a complication of mustard exposure, may complicate exposure to Lewisite.

Treatment for upper airway irritation is the same as for mustard exposure. Further complications of airway injury, such as pulmonary edema, must also be addressed as necessary.

- **Cardiovascular system damage**

Lewisite causes an increase in capillary permeability with resulting intravascular fluid loss, hypovolemia, shock, and organ congestion. This may lead to hepatic or renal necrosis with more prominent gastrointestinal effects that include nausea, vomiting, and diarrhea. With this loss in circulating fluid, careful attention to fluid balance will be an important issue.

PULMONARY AGENTS

Pulmonary intoxicants cause severe life-threatening lung injury after inhalation. These effects are generally delayed several hours after exposure. Treatment is usually supportive and may require advanced intensive care techniques including intubation, use of a mechanical ventilator in the hospital, and PEEP breathing. Pulmonary intoxicants included with this group are phosgene and chlorine.

PHOSGENE

Phosgene is widely used today in the manufacturing of dyes, coal tar, pesticides, and pharmaceuticals. It was widely used in WWI until mustard was introduced on the battlefield.

The Bhopal, India disaster of 1984 at the Union Carbide plant involved the release of 50,000 pounds of methylisocyanate, which is composed of phosgene and methylamine. There were 150,000 people affected, 10,000 severely injured, and 3,000 killed.

- **Characteristics**

Phosgene is a colorless gas above 47 degrees F and is 4 times heavier than air. It is generally transported in it's liquid state. As a gas, phosgene is colorless with and odor of sweet, freshly mown hay. It is principally a hazard by inhalation.

- **Decontamination**

With vapor exposure only, moving patient to fresh air should be accomplished quickly and clothing should be removed to prevent off-gassing. If liquid exposure occurs, areas of contamination should be removed with soap and water or flushed with copious amounts of water only.

- **Toxicity**

The primary damage from phosgene is from the carbonyl group. Phosgene dissolves slowly in water to form carbon dioxide and hydrochloric acid (HCl). In contact with upper airways, HCl causes a transient irritation of the eyes, nose, sinuses, and throat. A mild cough may also be present due to irritation of the upper airway and bronchi. There usually is a symptom-free period of 2 to 24 hours. Over the first several hours, the carbonyl group from the phosgene attacks the surface of the alveolar capillaries and causes leakage of fluid into the tissues. Eventually, this leakage of up to 1 liter per hour, causes severe hypoxia and apnea. A resulting severe non-cardiogenic pulmonary edema occurs.

CHLORINE

Chlorine is a significant irritant to the eyes and respiratory tract. It is widely used in the manufacturing of chemicals, plastics, and paper. It is commonly used in laboratories and in swimming pools. Industrial exposures have produced large numbers of injuries.

- **Characteristics**

Chlorine is found as an amber liquid or greenish-yellow gas that has a characteristic pungent odor. Although generally stored and transported as a liquid, when released, the resulting gas is about two times heavier than air.

- **Toxicity**

Chlorine injures cells by its reaction with water. Together with water, hydrochloric acid and free oxygen radicals are formed which attack cells. Chlorine gas is 30 times more irritating to the respiratory mucosa that Hcl.

Chlorine is toxic to any body surface including the eyes, skin, respiratory tract, and GI tract. In seconds after exposure, there are symptoms of irritation to the eyes and upper airways. This is followed by irritation of the respiratory tract which generates coughing, shortness of breath, wheezing, and sputum production. Initial respiratory distress is followed by noncardiogenic pulmonary edema in 12 to 24 hours after exposure. Sudden death is usually due to severe hypoxia and cardiac arrest.

- **Decontamination**

Exposed victims should be moved away from the source of exposure. Toxicity to skin and eyes should be flushed with copious amounts of water.

AMMONIA

Ammonia is widely used industrially in the U.S. with over 500,000 workers potentially exposed annually. It is used as an agricultural fertilizer and is used in the manufacturing of explosives, dyes, and plastics.

Ammonia is rapidly absorbed by mucosal surfaces and causes damage to the eyes, oral cavity, throat, and lungs. When mixed with water, it forms a corrosive agent, ammonium hydroxide which causes considerable damage in the form of liquefaction necrosis. Due to its high eater solubility, it penetrates tissues rapidly.

- **Characteristics**

Ammonia is a colorless, highly water-soluble, alkaline gas that has a pungent odor. Household ammonia has a pH < 12 and causes limited damage. Anhydrous ammonia, which is an industrial chemical, has a pH > 12 and causes severe damage.

- **Decontamination**

After the patient has been removed from the area of exposure, decontamination should be started immediately. Remove all clothing and wash with soap and large amounts of water for 15 to 20 minutes. The eyes should be irrigated continuously with water. A Morgan-lens device and topical analgesics will enable continuous eye irrigation therapy.

- **Eye damage**

Initially, ammonia causes burning, tearing, and severe pain to the eyes. Since it has a tremendous capacity to penetrate the eye, corneal opacification and lens damage leading to cataract formation usually occurs.

- **Airway damage**

Mild exposure causes cough, shortness of breath, chest tightness, wheezing, and laryngitis. Higher exposures can cause hypoxia, chemical pneumonia (pneumonitis), and hemorrhage. This will gradually improve over 72 hours. If the patient survives the first 24 hours, recovery is probable. Often times, higher exposures result in a non-cardiogenic pulmonary edema. Because of laryngeal swelling, early intubation should be considered to protect the airway.

- **Skin damage**

Pain, blister formation, and possibly deep burns similar to frostbite can occur.

- **Gastrointestinal damage**

If ammonia is ingested, severe mouth pain, cough, abdominal pain, nausea, and vomiting can occur. Severe edema of the lips and mouth is commonly seen. The patient should be observed closely to make certain that laryngeal irritation does not cause airway obstruction. Esophageal stricture and perforation is common.

BLOOD AGENTS

Blood agents are rapid acting chemical agents which can be lethal. They are usually seen in the form of a colorless gas or in the liquid state. The primary route of absorption is by inhalation. Blood agents poison the body inhibiting the enzyme cytochromeoxidase, thus interfering with cellular respiration.

CYANIDE

Cyanide is widely utilized, manufactured, and transported in the United States. It is used in printing, agriculture, photography, and in the manufacturing of paper and plastics. Cyanide is often transported via rail in 30,000 gallon tanks which makes it a potential threat for terrorism.

- **Characteristics**

Cyanide can be stored and transported in the liquid or solid state. As liquids, they vaporize at about 73 F and 58 C, so they will be in the gaseous from under most temperate conditions. It has been said that cyanide has a bitter almond odor, although it is undetected by 40% of the population. Large amounts of the chemical are needed to cause death.

- **Types of Cyanide**

The three types of cyanide that may be encountered are **hydrogen cyanide** (AC) and **cyanogen chloride** (CK), which are the liquid forms, and cyanide salts (sodium, potassium, calcium), which are the solid forms. Hydrogen cyanide has no irritant properties. Cyanogen chloride is a pungent, heavier-than-air vapor which can cause irritation of the eyes, nose, and throat. Salts are most dangerous following ingestion. Onset of action is slower and more prolonged. Cyanide salts generate hydrogen cyanide gas on contact with a strong acid such as sulfuric acid.

Cyanide exists normally in human tissues and is usually metabolized in the liver and excreted in the urine. Toxicity occurs when the cyanide binds to iron in the mitochondria which prevents the cell from using oxygen. Without oxygen, cells begin to die. The heart and brain cells are affected initially.

- **Toxicity**

Acute cyanide poisoning occurs after inhaling the agent, drinking solutions of cyanide or by skin contact with large amounts of liquid cyanide. After inhalation of a low concentration, the patient becomes anxious, begins to hyperventilate, may complain of dizziness and headache. Vomiting may also occur. A flushed or "cherry red" appearance to the skin may be seen, although it is uncommon. Symptoms improve once the casualty is moved away from the source. Symptoms should not progress but should improve once exposed to fresh air.

In contrast, after inhalation of a large amount of cyanide, approximately 15 seconds later, the victim becomes anxious and starts to hyperventilate. Thirty seconds after exposure, the victim may begin to have seizures. Three to five minutes following exposure, breathing ceases and in 6 to 10 minutes, asystole and death occurs. Initially there is absence of cyanosis and the patient may have normal sized or dilated pupils.

Patients will appear in respiratory distress but have a normal O2 saturation. Metabolic acidosis, usually a lactic acidosis, will be present on ABG results due to the lack of oxygen to the tissues.

Cyanide toxicity can be measured by serum cyanide lab studies. However, there may be a delay of several hours in obtaining these studies.

Fundamentals of Encryption

by

Nick Lafleur

One of the most feared actions surrounding the Internet and computer community is data loss or theft and system intrusion. Many systems are the target of malicious attacks either by in house employees or third party individuals or corporations.

Understanding the sometimes overwhelming cost of full blown protection used in cooperation with firewalls, proxies, vpn's (Virtual Private Networks) and the like, the average to moderate user often takes a more definitive approach to personal computing security. Rather than protecting an entire network system, or systems, a user can protect one computer, or a single piece of information, either for storage or Internet travel to other users via email.

The home and business user alike can use encryption to protect a variety of media and can do so at varying cost from free software to modestly priced programs.

Encryption is one of many protection methods and currently one of the best from small to medium scaled information protection. It can, by user choice be utilized to protect larger media as well.

Encryption is simply a method used to protect files, folders, drives, email, and various other media from intrusion, theft or detection by using various algorithms to "scramble" the intended material. Once the proper password is used, the program will then "descramble" the material back to its original state.

While encrypted, the material is viewed as an indistinguishable combination of characters that are extremely difficult (not impossible, however) to compromise. At present, encryption provides the maximum amount of protection for sensitive material.

A common encryption program PGP® (http://web.mit.edu/network/pgp.html) or (www.nai.com) is described below. Note that this is not an endorsement or advertisement of this product, it is however a description of what is quickly becoming the industry standard in encryption.

Example:

User A has an encryption software program, which is used to encrypt certain material. The user sets up a private "key" and a public "key" protected by a password and used for the purpose of encrypting/decrypting anything from a single file to an entire hard drive. The public key is stored on the users computer and on an Internet database for retrieval by other users, which the original user denotes (authorized users). A private "key" is stored on the original users computer for his/her own use and is neither the same, nor is accessible by any other person.
Using the private "key" the user encrypts the material for transfer to another user. In most cases, the intended party must have the same encryption program (many are free). The intended party then uses the original users public decryption "key" (obtained either from the user, or from an Internet database), decrypts the material and proceeds. It is important to note that a third party cannot use the original users "key" to decrypt the material without being listed as an authorized user.

This example is one of many, and several resources on the Internet provide more extensive background to encryption. In addition, other software exists that merely password protects the material with simple to advanced methods, and varying from simple to advanced encryption.

The following sources provide information and download of many security related utilities. Additionally, anyone interested in security related programs will find abundant information by conducting an Internet search using the keywords "security utilities" or "encryption"

http://www.winfiles.com/apps/98/security.html A large site with many sections of downloadable software.

http://nonags.gargantuan.com/security.html A site with a large section of free downloadable software.

http://nai.com The Network Associates® web page, with information on PGP® and other security info.

Computer Viruses and Solutions

by

Nick Lafleur

Viruses, within the computer usage spectrum are program, commonly small in size, that are written to change the operation of a computer or system. The goal is to accomplish this without the permission or knowledge of the owner. Viruses accomplish two tasks. First, they execute themselves once the program or file is opened, often embedding their own code in another program. Second, they replicate themselves onto other disks or into other files. A virus can spread from a single file on a single computer to any and all computers on a network once the initial execution is accomplished. Additionally, using the internet, a virus can spread to anyone who's email address is located on the host computer, thus infecting multiple users.

When dealing with viruses, there are essentially 3 types or categories that are represented: program, boot and macro.

Program viruses infect program files. Files with the extension exe, com, dll, drv, sys, bin and bat are common program virus targets.

Boot or Boot Sector viruses infect the system data area of a hard or floppy disk. Computers have a boot sector on the root drive that has certain instructions on how the system should start up and initializes during startup, in a like manner, when booting from a floppy, such as when installing an operating system or recovering from a crash, information on the floppy boot sector is vulnerable to boot viruses. The virus would attach itself in this system area and initialize while the system is booting up. Once a virus exists in memory, every time a floppy or file is accessed, the virus checks to see if it is infected, if that file or disk is not infected, it then proceeds to spread. This is done each time access is attempted to any floppy disk or hard disk. Attention is decreasing to boot viruses which actually makes them more dangerous, since viruses types have no "trends" denying attention to a certain type just makes it that much easier to get infected. Once way of avoiding boot viruses is to make sure no floppy disk is in the floppy drive during system startup. Since boot viruses are most often taken from floppy disks, keeping your drive empty during startup will afford a measure of protection.

Macro viruses are indigenous to Microsoft Office programs (Word, Excel, PowerPoint and Access files) This is a starting point for macro viruses, as they too are spreading to other types of programs. Macros are automatic commands that are written on the fly within a program using that programs language. Their task is to speed up and automate common tasks. Macro viruses then would infect a macro and execute upon that macros use. The possibilities are almost endless with macro usage.

Viruses spread by being executed. It is a common misconception that viruses simply initiate themselves. Instead, the program or file that is infected must be opened or ran, at this time the virus will start up and from there can replicate or otherwise spread. Downloading an infected vile via email will not infect a users computer until the infected file is open or ran. A user will run a program that is infected, which in turn will initiate the virus which loads itself into memory. From then on, the virus will infect other programs or files, or accomplish whatever task it was designed to.

Boot viruses commonly are spread when a user attempts to boot the system using an infected floppy disk in the floppy drive. Once ran, the virus writes itself into the master boot record and infection propagates from there.

Viruses design vary with each writer, but commonly they are used to 1. Annoy 2. Destroy or 3. Burden resources. A virus may simply show messages in video, audio or text form to the user for a period of predetermined time, or perpetually until the virus is destroyed. Viruses can also destroy or corrupt files, folders, programs or entire hard disks. Viruses burden system resources by sometimes using up too much system memory until the system is functioning below specified parameters due to the overuse.

Email is also a preferred way to disseminate viruses. Programs or files from the internet can be altered to contain a virus and thus downloaded by the general public. Normally, downloading email with a file attached that is infected cannot harm you, but Microsoft Outlook and some other programs can "auto" run attachments which makes the risk of infection extremely risky. Outlook also has a Microsoft acknowledged security vulnerability that will allow certain viruses to auto run without user intervention. If you use Microsoft Outlook, be sure to check the Microsoft website for the patch created to fix the security hole. When downloading email, check to see if the person who sent you an attached file is known to you, if he/she is not, then do not open the file without scanning it with an Antivirus program. Check for common taglines in the subjects of emails. Common taglines included with popular viruses are: "here is the file you requested" or "special message for <your name>" or "Vacation pictures you wanted" and the like. The previous are actual taglines taken from existing viruses but these can and will vary.

Even if that user is known to you, attempt to discern if that user is generally safe with files or simply downloads and passes any file on to their friends. When in doubt, always scan for viruses. Anyone who is very active with email should have a utility that scans email attachments for viruses. Everyone, no matter what their level of use should have Antivirus software running on all of their systems.

Trojan horses are not really viruses, but are commonly referred to as such. Trojans are simply not viruses because they cannot replicate themselves. Essentially, a trojan horse is a malicious program hidden inside of a normal or desirable program. An example would be if you downloaded a cartoon screensaver from a website and were infected when you ran it because of malicious code written into the screensaver code.

Worms are viruses that replicate without using a host file. A worm would be embedded into a file and the entire file would be the virus and spread from computer to computer. This is common in picture files or joke lists and the like. They spread in their unaltered form from system to system containing the virus within their code.

Public download sites and BBS's are at great risk from virus dissemination due to the large numbers of users who frequent these sites. Once site could see thousands of users in a normal days traffic, which could in turn spread one small virus to thousands of computers from one location. Many viruses are taken from public forums, pornographic sites and newsgroups. Some even masquerade as free software that you would otherwise have to pay for, also known as warez. Generally, a good antivirus program and some common sense when using the computer will prevent a user from serious data loss and possible unrecoverable problems.

The single best way of preventing data loss is by backing up your important data and taking it out of the computer and onto a zip disk or floppy that is prescanned and then write protected. Write protection after the data is backed up on the disk makes sure that nothing else can write to the disk, including viruses. You do not have to back up programs, since you should have the installation disks for your system handy, and programs can be reloaded easy enough. The files that you created with each program should be stored on external media and protected.

The following links will provide some information on data protection and antivirus solutions.

www.symantec.com	Creators of Norton Antivirus software
www.mcafee.com	Creators of McAfee VirusScan software
www.iomega.com	Makers of external/internal backup and storage media
www.syquest.com	Makers of external/internal backup and storage media
http://www.umich.edu/~virus-busters/	Information on viruses and hoaxes

Understanding the Impact Of Biological & Chemical Terrorism

by

Wade M. Knapp, CPS
Lee A. Knapp, RN, CEN

Outside of a few professional groups and the United States Military, there is a very poor understanding of biological and chemical weapons and their effects. Few civilian law enforcement agencies, emergency responders, or hospitals are prepared for, or even understand, the devastating effects that can occur within a community if one of these weapons is released. This reality creates an enormous risk to public safety, not to mention the risk confronting the emergency response community. While it is true that a large scale incident involving the use of a biological or chemical weapon has not occurred in the United States, we should not use that fact as a reason not to prepare. The shear nature of terrorism dictates that we will probably never know in advance when or where an incident may occur. We should not presume that advance warning of a terrorist attack will be given. In addition, we probably will not know the type of biological or chemical agent used until after the attack has occurred. Because the time and place of the attack, and the weapon to be used is under the control of the terrorist, he or she will usually have the advantage over us. Because of this fact, we must prepare for the worst, and hope for the best.

Due to the nature of a biological and chemical weapon attack our response planning must address two fundamental aspects. First, response plans must be developed through a viewpoint of public health . These types of weapons do not destroy buildings, they infect or contaminate people causing illness, injury, or death. The second aspect is one of general public safety. Government and law enforcement agencies must understand both the physical and psychological impact that this type of incident may have on the general public, as well as the overall security of the environment. Although the mechanisms of action may vary slightly between biological and chemical agents, the results are usually the same; large numbers of medical casualties. We will first examine how such an event may effect the community from the aspect of a terrorist act involving a biological weapon agent.

Properly disseminated, the effects of biological warfare agents may not be seen for days, or even weeks, after the initial attack has occurred. This is due to the incubation period associated with biological organisms. This fact makes biological terrorism much harder to detect. Theoretically, a terrorist could disseminate a biological agent infecting a civilian population, escape afterwards, and be on the other side of the globe before we even knew what happened. Once the effects of the agent begin to surface in the community, it is possible that large numbers of people will have been infected, become symptomatic and seek medical attention. The numbers of infected people would depend upon the type of biological organism used. For example, it has been estimated that the proper dissemination of as little as one pound of Anthrax would be enough to kill the entire population of a major city. Fear and panic among the population is a very real possibility that must be considered following such an incident. An effective method of disseminating public health information would be necessary to inform the public as to what action is being taken, and where to seek medical attention.

In order to respond effectively to such a public health disaster the need for extensive and prolonged medical services would be required. The ill would be self-referring to local hospitals, personal physicians' offices, pharmacies, etc. at an alarming rate. Local Emergency Medical Service providers may not have adequate personnel or ambulances to respond and transport all the victims calling for assistance. There would be an increased need for Personal Protection Equipment, medications, medical and other support equipment that may not be readily available in the aftermath of the incident. Hospitals will experience overcrowding not just from the truly ill victims, but also from many unaffected people that have various nonspecific symptoms, or fear they are infected.

In the event that large numbers of patients, exhibiting similar symptoms, present to local Emergency Departments within a short period of time, Emergency physicians need to have a high index of suspicion that an attack using biological agent has occurred. The same holds true for private Physician's offices receiving unusually large numbers of patients exhibiting similar symptoms. Consequently, disease onset in a community would be rapid and treatment would need to be implemented quickly to have any effect on mortality, or to ensure effective prophylaxis, by implementing PPE, antibiotic therapy, or vaccinations if available.

Some biological agents are communicable, some are not. In an incident involving a communicable agent, an ordered quarantine may be required to stop the possible spread of disease. Non-communicable agents generally do not require quarantine. The possibility of a quarantine following a biological weapon attack may exhaust both hospital and public health resources and personnel. Law enforcement agencies may also become taxed by assisting with an ordered quarantine, in addition to maintaining public order and conducting an investigation into the incident. Problems would also arise with the handling and storage of the deceased, requiring the need for additional mortuary facilities.

The second scenario we will examine is the possible effect to the community caused by the release of a chemical warfare agent. In general, the effects are similar to that of an incident involving the use of a biological agent with a few exceptions. Chemical warfare agents are disseminated in much the same manner as the biologicals, with the primary route of exposure being inhalation or absorption. The effects of chemical agents are generally more rapidly occurring than biological agents. The effects of a chemical agent may appear within minutes to hours after contamination. Since the effects of chemical agents occurs quickly, identification of the site of release is more easily located. Police and emergency responders should be able to isolate and secure the scene after evacuating people from the area. Having the ability to quickly locate, and isolate, the site of release should limit additional exposure and aid in the investigation process.

If properly disseminated, the effects of a chemical warfare agent would occur quickly and produce large numbers of contaminated casualties at the site of release. The specific effects produced would depend upon the agent involved. These effects may, or may not, be immediately incapacitating in nature. Fear and panic among the victims effected should be anticipated. Winds may carry the agent beyond the site of release, contaminating others. The need for extensive medical services and decontamination at both the site of agent release and local hospitals will be required. In addition, there will be an increased need for Personal Protection Equipment (PPE), medication and antidotes, decontamination and other support equipment that may not be readily available in the aftermath of the incident.

The possibility of a quarantine for chemical agents may not be necessary due to the non-communicable nature of these agents. However, cross-contamination from man to man is possible with many of these chemical agents. Problems may still arise with the handling of the deceased and the need for additional mortuary facilities. Hospitals will experience overcrowding not just from the effected victims but also from many unaffected people that have various nonspecific symptoms and believe they may have been contaminated. Emergency response personnel and police would likely be taxed throughout the initial phases of the incident due to the large numbers of victims requiring assistance. However, the situation could improve in as little as a few hours considering the non-communicable nature of chemical agents, and if no additional attacks occurred.

These scenarios are fundamental illustrations of how a community may be impacted by a terrorist act utilizing biological or chemical weapons. It should be remembered that the points outlined in this text only partially portray the problems which might be encountered during one of these types of incidents.

Using Passwords In A Computing Environment

by

Nick Lafleur

Passwords are a common tool used in the protection of files, drives, directories or single information sources. Operating systems such as Microsoft Windows® or Linux® have their own moderate levels of password protection. Outside sources also provide software designed to password protect or encrypt data. One such piece of software that will be discussed later is PGP (Pretty Good Privacy) with features such as single file or full drive encryption, this software utilizes some of the best encryption technology available today. In addition, software encryption or password programs generally provide varying levels of protection, as well as allowing multiple users to protect different files unique to the user. In this paper, we will look specifically at passwords.

The key to passwords is using the intended software's full capacity. For example, if the number of digits the software uses for a password is 8, a user should pick a password using the maximum allowable length for best results. Generally, depending on the type of software, or what it is designed to protect, users can expect to find between 4 to 16 characters for the password.

A user should pick a password that is unique, and never write the password down somewhere that would enable someone else to find it.

Proper usage dictates using alphanumeric characters whenever possible. Depending on software limitations, you should use sporadic passwords containing letters and numbers in no fixed pattern.
For example, the 17 digit password "b182azx332xsa9204" is less likely to be compromised than the password "freedom". Once again, depending on software limitations, you may have to use less characters, but all should be in no fixed order, and not pertaining to anything tangible that would be associated with the material protected, or the user.

Recommended updating of the encryption/password software should be done whenever new versions are released. Changing passwords should be done about once per month, depending on the sensitivity of the information being protected. Try not to use the same password for different encryption/protection, or for different files/folders/drives. Using unique passwords for each desired protection enables a more secure design.

Listed below are examples of what **not** to use when deciding on a password. This list is the opinion of the author but it should be noted that a good password cracker, or program, will more than likely use the following guidelines when trying to break a users password.

Try Not To Use

- Birthdays or combination of birthdays of any family member.
- Corporate inception dates, or dates of importance.
- Family names in any order.
- The word "password"

- The numerical sequence “1234” or any related sequential numbers.
- Mother’s maiden name. (this is a favorite of credit card companies)
- Holidays, Anniversaries, or Historical dates
- Passwords used by previous users of the same system
- Any other entries which immediately come to the users mind, or which can be guessed by looking around the room where the system is located.

In conclusion, users should be aware that passwords are a first line of defense in securing material, but only a part of the overall security process. Never assume that one piece of equipment, one type of protection, or one manufacturer can provide total security in any field. The intrusions are as varied as the software, so as an overall security plan, be sure to research new updates and patches to current systems and software. 100% security is virtually impossible, but users can shift the balance of power to their side by keeping in tune with the ever-changing security management techniques that encompass total system protection.

Telephone Bomb Threat Procedures

by

Wade M. Knapp, CPS

Receiving a bomb threat over the telephone can be a stressful situation. The bomb threat call will usually come without warning and require immediate action on the part of the person handling the call. No matter how much training you've received in handling these calls, each threat will be unique and require your complete attention. While it is true that the vast majority of telephoned bomb threats are hoaxes, they must be considered real until proven otherwise. Being on the receiving end of a bomb threat call will demand the use of all of your interpersonal skills, as well as, your professional telephone skills. Concentration, professionalism, active listening, note taking and asking questions will all be necessary if one hopes to obtain all possible information from the caller. The following is a list of important points to remember if you receive a bomb threat call:

Remain calm and in control. Panic and fear can interfere with your ability to concentrate and in turn cause you to miss valuable information the caller may have to offer.

Don't hang up, transfer the caller or place the caller on hold. This may be the only contact the caller will have with the facility. If you hang up on the caller, they may not call back. If you transfer the caller or place the caller on hold, they may not be there when the line is picked up again.

Signal a co-worker to listen in on another extension. The co-worker may pick up on information you miss during the call. If a co-worker does listen to the conversation over another extension it is important that they take notes and not speak to the caller. If two people are speaking to the caller at the same time, it may confuse or anger the caller or be considered as a lack of respect or trust.

Signal a co-worker to notify security or management. It is important to initiate the bomb threat response plan as soon as possible.

Use all your telephone etiquette skills. Be polite and treat the caller with respect. Don't talk with others around you while on the line with the caller. Don't become angry, degrade or verbally abuse the caller. Angering the caller may cause them to terminate the call before the necessary information can be obtained.

Keep it conversational. Try to get the caller to talk and keep them talking as long as possible. The more the caller talks, the more information you'll be able to get. This may require you to talk also. Ask questions. Obtain as much information as you can.

Obtain all important information. While all information given by the caller is important, the three most important pieces of information to obtain are:

WHERE IS THE BOMB?

WHEN WILL IT EXPLODE?

WHAT DOES THE BOMB LOOK LIKE?

If the caller does not volunteer this information, ask for it. Unless you are able to obtain this information, little can be done to respond to the threat. When you obtain this information, repeat it back to the caller to insure it is correct.

Take notes during the call. Write down everything the caller says. Have a bomb threat checklist at your desk at all times.

Pay attention to background noises on the telephone. Listen for music, sounds or any other noises that could give a clue to where the call is coming from.

Pay attention to the caller's voice. Does the caller have an accent or speech impediment. Is the caller male or female? Does the caller sound like an adult or child? Does the voice sound familiar?

Recognizing Letter And Package Bombs

by

Wade M. Knapp, CPS

Incidents of explosive devices arriving as mail have been occurring in the United States since the end of World War I. However, it must also be noted that incidents of explosive devices arriving in the mail are very rare. Only a handful of incidents involving letter or package bombs occur annually in the United States. The problem is you can never predict in advance where and when one will arrive. Letter or package bomb incidents have occurred at businesses, personal residence, universities, government building, etc. Generally, explosive devices shipped through the mail are not random acts of violence, but very personal acts of violence. The perpetrators of letter or package bomb attacks usually have a specific target in mind to receive the bomb. The motivations for this kind of attack could include revenge or other personal grievance, protest, or insurance fraud. Organizations concerned with the threat of mail bombs should develop bomb security planning that includes mail screening procedures, bomb threat procedures, evacuations, etc.

Utilizing mail or package services as a method of bomb delivery may be a desirable tactic for terrorists or criminals for several reasons. Sending a bomb through the mail allows the bomber to attack a target over great distances without personally traveling to the target's location. No potential target is outside the reach of mail or package services. In addition, utilizing the mail or package services as a delivery method may reduce the bomber's risk of capture.

This method of bomb delivery also presents some risk for the bomber. Once the bomb is mailed, the bomber loses control over what happens to the device. The device could be discovered during handling by postal employees, could detonate prematurely killing or injuring the wrong people, or because of some problem with the package, be returned to the bomber undelivered. Even if the bomb reaches its intended target, modern forensic and investigative techniques utilized by Law Enforcement agencies have been very successful at linking bomb devices to the individual that made the device. But even with these risks, mail bombing still remains a viable tactic for terrorist and criminals who choose to use bombs as a weapon.

As long as mail bombing remains a viable terrorist tactic which can be used against an organization and its personnel, counter-tactics should be utilized to reduce the risk of a mail bomb occurrence and handle the situation if it does occur.

Recognition Clues For Letter or Package Bombs

The early detection of a letter or package bomb, before it reaches the intended recipient, is the goal of a mail bomb security program. Mail room employees, or others which process the mail, should do so using caution and an established screening procedure. Individuals processing the mail should sort and inspect mail in a manner that allows them to pick up on the recognition clues or "warning signs" of a potential mail bomb.

Recognition clues are abnormalities in letters and packages that raise suspicions that the letter or package may be something other than what it seems. These recognition clues have been assembled from evidence in previous letter and package bomb incidents. Letter and package bombs can be designed in any number of configurations and contain a variety of components. The way in which letter and package bombs are designed generally contributes to the type of recognition clues which may be present. Mail bombs may have one or more visible recognition clues. However, it must also be said that letter and package bombs may not have noticeable recognition clues. A letter or package bomb may appear to look like any other piece of business mail.

Individuals sorting and inspecting mail should look for these recognition clues no matter what the source of the mail. One clue found on a piece of mail may not be enough to justify suspicion, but multiple recognition clues on a single item of mail should raise suspicion greatly. The following is a list of basic recognition clues:

- **Foreign Mail**
  Letters and packages arriving from foreign countries. This may be indicated by the return address, foreign post marks or stamps. Does the company normally send or receive mail from other countries? Is the individual or company sending the letter or package known?

- **Special Deliveries**
  Deliveries from parcel services, courier services, private companies, deliveries of flowers or gifts, or other such hand deliveries should be verified as legitimate deliveries.

- **Abnormal Deliveries**
  Deliveries left during non-working hours. Deliveries arriving late at night. Deliveries by persons who do not appear to work for a parcel service or claim to be a friend of an employee working for the company.

- **Professional Packaging**
  There is generally a visual difference between letters and packages sent from corporations and those sent from the general public. If the labeling states the package is from a corporation the packaging should reflect a professional appearance.

- **Restrictive Markings**
  Markings such as “Personal”, “Confidential”, “Private”, or other such wording. Words like these suggest the envelope or package should only be opened by the person to whom it is addressed.

- **Addresses Hand Written Or Poorly Typed**
  Letters and packages arriving from corporations normally contain professional labeling.

- **Incorrect Titles**
  The titles of company officials are listed incorrectly on the envelope or packaging. This may demonstrate a lack of knowledge of the company’s corporate structure.

- **Titles But No Names**
  Letters or packages listing a company official by title only.

- **Misspellings**
  Misspellings of common words, addresses, states, etc. This suggest a possible difficulty with the English language or that the item was not mailed by a corporation

.

- **Oily Stains Or Discoloration On Packaging**
  Envelope or packaging has stains, discoloration or is damp to the touch.

- **No Return Address**
  No return address is listed on the envelope or packaging. Legitimate business correspondence normally has a return address listed.

- **Excessive Weight**
  Envelope or package weighs more then it should for its size. The weight of the letter or package arouses questions as to the contents. The letter or package weighs more than it could if it contained only paper.

- **Excessive Postage**
  Envelopes or packages affixed with more then the required postage. Excessive postage would be used to insure that the letter or package was delivered. Odd combinations of postage stamps or foreign postage stamps may be a clue.

- **Rigid Envelope**
  Envelopes feel stiff, rigid, contain heavy cardboard, metal or plastic rods or other objects meant to keep the envelope from bending. These types of reinforcements may be used in an attempt to prevent the device from being damaged during shipment.

- **Package Is Uneven Or Lopsided**
  Weight or contents of the envelope or package is unevenly distributed or feels lumpy. Bomb components can come in a variety of shapes, sizes and weights and the combination of components could create this uneven or lopsided effect.

- **Protruding Wires Or Aluminum Foil**
  Wires or aluminum foil protruding from envelopes or packaging should be considered suspect.

- **Excessive Securing Material**
  Envelope or package is sealed with an excessive amount of tape or string. The amount of sealing material seems odd compared to the size or weight of the envelope or package. The package has been sealed in a manner that would prevent it from being accidently opened.

- **Visual Distractions**
  Packages wrapped as Christmas presents, have other holiday markings, packaging contains drawings, symbols or stickers, etc.

- **Package Has Strange Odor**
  The envelope or package emits a strange or chemical smell.

- **Sounds Coming From The Package**
  Sounds of ticking, buzzing, clicking or any other strange noises should be considered suspect. They may be noises from a timer or clock attached to the device.

- **Inner Enclosures**
  When the package is opened an inner (secondary) enclosure is found.

Discovering A Suspected Mail Bomb

The goal of mail screening procedures is to detect a possible explosive device concealed as an article of mail before it injures anyone. Most people handle mail every day of their lives and very few have ever received a letter bomb. Unless every piece of mail is being x-rayed, common sense and good judgement, on the part of the personnel screening the mail, must be applied at all times.

When a piece of mail has been determined to be suspicious, the primary concern should be your personal safety and the safety of your co-workers. No further action should be taken to deal with the item beyond its discovery. The fact that the item has not detonated should not be a reason for further risk to personal safety. Law Enforcement agencies employ personnel trained to handle such situations and they should be notified at once. When a suspicious item of mail is discovered, the following action should be taken:

Remain calm.
Set the item down immediately.
Don't handle or move the item.
Don't cover the item.
Don't place the item in water.
Don't attempt to carry the item outside.
Don't permit others to handle the item.
Notify management and co-workers of the discovery.
Evacuate the area.
Notify Law Enforcement.
Once the area has been evacuated, do not permit re-entry to the area.

When Law Enforcement officials arrive, provide information regarding the location and description of the item, along with what action has been taken.

Understanding Crime Risk Management

by

Wade M. Knapp, CPS

Developing an effective crime prevention program requires some careful thought and detailed planning. Businesses must be able to identify and understand those risks which confront them. They must be able to accurately determine their probable exposure to such risks. They must have an understanding of their current level of protection, and evaluate the need for improved measures. Normally, the most effective method of evaluating one security program is to have a Security Survey conducted by a professional security auditor. And finally, these improvements, if any, must be incorporated into the current security and safety program. The key to effective risk management is planning.

Understanding Crime Risk

Before a crime risk can be identified, reduced, or prevented, we first must have an understanding of what a crime is. A crime can be defined as: the commission of an act which violates an established law. This is the definition of crime in its simplest terms. However, we must realize that while the concept of crime is simple, the true nature of crime is much more complex. Millions of crimes occur annually in the United States. On the surface, it would appear that all of these crimes have very little, if nothing, in common with each other. However, under closer examination we will find that these crimes have more in common with each other than we think.

A crime is the product, or result of an individual's criminal behavior. Human behavior is never a random occurrence, but a specific action which has a definite goal in mind. People basically think and act in much the same manner both psychologically and physically. We all have the same basic emotions, reactions to physical discomfort, we walk and talk, we have desires, needs, and goals, and a host of other similarities. These behavioral similarities can be identified and modeled because they occur within a structure. The only exception to this rule may be those individuals who suffer from genetic psychological disorders, or persons suffering from diseases that damage the brain's functions.

Since criminal behavior is a human behavior, we can assume that it has a structure to it as well. And if you assumed this to be true, your correct. There are certain common aspects, or elements, which are present in criminal behavior, as well as, criminal acts. This is not theory, but scientific fact. Criminals behave and operate in much the same way, even though they may have nothing else in common with each other. However, another aspect of human behavior which must also be given consideration is, human behavior is difficult, if not impossible, to predict in advance. Generally, we have no way of knowing when or where the next crime will occur, or who will commit that crime. This is the aspect of crime which is interpreted as randomness. Beyond this fact, once a crime has occurred, certain elements of the crime will be common and consistent with others, even though no two crimes are the same. These elements include such things as: motivations, methods, criminal histories, tools or weapons used, types of evidence left at crime scenes, etc.. These commonalities are what forensic science refers to as the elements of the crime. It is this common structure of crime that needs to be dissected and studied in order to obtain a better understanding of these acts. All criminal acts possess three fundamental elements: **desire, ability, opportunity**.

Desire

An individual must possess the desire to commit a criminal act before one can occur. Desire can also be called **motivation** or **intent**. Desire is the psychological element of the criminal process. An individual's motivation for committing a crime could be financial gain, revenge, a political agenda, a fantasy driven by a psychopathic disorder, or any number of other motivations. Since the desire to commit a crime stems from a psychological or emotional process, it is very difficult, if not totally impossible, to control or predict it. No one can realistically control or predict another persons thoughts or emotions, and it's these very thoughts and emotions that will drive the criminal act. The most we can realistically do, is attempt to influence an individual and hope that they convince themselves not to commit a crime.

Ability

An individual must also possess the ability to commit a crime. Possessing the ability to commit a crime means the individual must have the necessary **physical capabilities**, **skill**, **knowledge**, the **proper tools**, etc. This element in the criminal process is also difficult, if not impossible, to control. In our society, there is no way to realistically control an individual's physical capabilities, capacity for learning or developing skills, the instruments he / she has access to, availability of information, etc.. Developing the physical abilities which could be utilized for criminal activity, in and of itself, is not the problem. It's when these abilities are combined with the desire to commit criminal acts that it becomes a problem.

Opportunity

The last element in the criminal process is opportunity. An opportunity to commit a crime must be present, before one can be committed. This means there must be a target of the criminal act. This final element of the criminal process is one that we do possess some degree of control over, because criminals don't select targets by accident. There is a structure to the way in which criminals select their intended targets. Criminals select their targets based on a specific criteria. This target selection criteria is based on four key elements:

> **Suitability**: the criminal must consider the target to be suitable for his needs.
>
> **Vulnerability**: the target must be vulnerable to the criminal's attack.
>
> **Accessibility**: the criminal must be able to gain access to the target for the amount of time necessary to commit the act.
>
> **Risk present**: the criminal must consider the level of risk associated with the commission of the crime. Will he / she be able to escape after committing the crime, what level of resistance will be confronted, will the police interdict? These are all aspects that will be considered prior to committing the crime.

It is important to understand the relationship between this target selection criteria and opportunity. If this selection process is the basis for choosing the right opportunity to commit a crime, and our goal is preventing the crime. We should then examine how we can interfere with this selection process in a way which reduces the likelihood of the crime occurring.

Potential targets can be classified as either "**soft targets**" or "**hard targets**". Soft targets are ones in which minimal, if any, protective measures are employed to defend against criminal attack. Hard targets are ones in which extensive protective measures are employed to defend against criminal attack. Statistically, soft targets are attacked more often, than are hard targets, due to their vulnerability to the attack. In general, criminals would rather attack a target which is less prepared, than one that is on the defense against such activity.

Reducing potential vulnerability by increasing protective measures may be most effective method of preventing criminal attacks. If we increase our levels of physical, technical, and procedural security measures we become a harder target to attack. This increase in security should result in limiting access required to the target, as well as, increasing the risk the criminal faces. The less vulnerable we are to a criminal's attack, the less suitable we are as a potential target. The ultimate goal is to become an unsuitable target. This goal can only be achieved through the application of specific risk management principles, in systematic and realistic manner.

Principles of Risk Management

Most crime risks, and accident risks as well, can be reduced to some manageable level through the application of one or more of the following risk management principles:

Risk Avoidance

Risk avoidance means that if the object at risk is removed completely from the threat environment, the risk will be avoided. For example, if you were concerned about the threat of theft of a valuable coin collection maintained in your residence. this risk could be avoided if the coin collection was removed from the residence and secured in a bank safety deposit box.

Risk Reduction

If the object at risk cannot be completely removed from the threat environment, than measures must be taken to reduce the threat. Reducing risk can be accomplished through the application of physical, technical, and procedural security measures.

- **Physical Security Measures**, are considered those things which create a physical protective barrier around the object at risk. Typical physical measures include: fences, gates, walls, barricades, doors, windows, locks, safes, bullet resistant glass, Security Officers, Security Dogs, etc.

- **Technical Security Measures**, are considered those things which operate electronically and include: alarm systems, CCTV, electronic ID card reading access control systems, bio-metric access control systems, lighting, etc.

- **Procedural Security Measures**, are those routine actions we take to either prevent, or respond, to crime. Protective procedures can include: security patrolling, establishing safety and security policies, checking ID cards or other forms of access verification, auditing and inventory control, cash depositing, giving sales receipts, escorting employees to their cars, evacuations, managing a crime or accident scene, report writing, or any number of procedures which may be utilized to enhance security and safety.

Risk Transfer

The objective of this principle is to transfer a potential threat to someone or something else. The most common form of risk transfer is to insure the object at risk. By insuring the object, it allows you to recover financially from an attack. The potential loss resulting from a criminal attack is transferred to the insurance company.

Risk Acceptance

Lastly, it should be realized that the possibility of completely eliminating risk can never be truly accomplished. There is no guarantee that a risk will not manifest itself, no matter would measures are taken. This is a simply fact that must be understood and accepted.

The application of these risk management principles won't completely eliminate the possibility of crimes or accidents occurring. However, it should allow for the reduction of the likelihood of these incidents occurring. The extent to which any individual risk management principle, or combination of principles, is applied will depend upon what is being protected and the level of threat in the environment.

Security Patrol Operations

by

Wade M. Knapp, CPS

Security Patrol can be defined as "the act of moving about an area with the goal of providing protection, enforcing rules and conducting observations." Patrolling should be considered the hallmark of the security industry and the Security Officer on patrol the very backbone of the profession. Because an effective protective operation cannot be achieved from the position of sitting behind a desk. Patrols are necessary to insure the integrity of the overall security program. Safety and security problems occurring within the protected area of operation need to be discovered and corrected in a timely manner. This can only be accomplished if someone is actually physically patrolling the area with that purpose in mind. Security patrol operations are conducted for a variety of reasons including:

- Crime prevention.
- Enforcement of company policies.
- Fire safety.
- To provide assistance to personnel.
- Identification of hazardous situations.
- Protection of personnel.
- Assisting with medical emergencies.
- Detecting failures in facility operations.
- Protection of company property.
- Visitor / Vendor access control.
- Equipment inspections.
- Creating a positive image for security.

The function of security patrolling requires common sense, skill, diligence, and discipline on the part of the Security Officer performing the task. The Security Officer must be able to adapt to a wide variety of patrol environments and situations. The Security Officer may find himself / herself conducting patrol operations in locations such as construction sites, retail establishments, industrial facilities, marine vessels, office building, public events, or any other place which requires protection. In addition, the Security Officer must also adapt to the ever-changing weather conditions such as, the heat of summer, the cold of winter, rain, wind, fog, etc. Patrol operations can also occur during daylight hours, as well as in the darkness of night. Patrolling also creates the possibility of encountering people engaged in situations ranging from normal daily activities, to situations of physical distress, or possible criminal conduct. Because of this reality, it is important that the Security Officer be knowledgeable, skilled, and prepared if the mission of the patrol operation is to be successful.

Methods of Patrol

There are two basic methods of patrol common to the security industry. These patrol methods are foot patrol, which is the most common, and vehicle patrol. In some instances, security operations may utilize other methods of patrol such as bicycle patrol or horseback patrol. These types of patrol are not that common in the security industry, and require specialized training prior to the Security Officer utilizing such patrol methods. For this training program, we will concentrate on the two most widely used patrol methods, foot patrol and vehicle patrol.

- **Foot Patrol**

The traditional method of security patrolling is the foot patrol. Nothing can replace the effectiveness of the trained Security Officer walking a patrol route with the purpose of detecting abnormal situations.

By conducting security patrols on foot, a Security Officer has the ability to inspect virtually every square foot of the site in which he is assigned to protect. Having the ability to make such detailed inspection of a facility or area, is a valuable part of any good security program.

Another aspect, which is of great benefit to any company requiring protective services, is the flexibility offered by foot patrolling. Foot patrols can be conducted inside building, on the grounds located outside a building, during the daylight or nighttime hours, or during times of adverse weather conditions. A Security Officer patrolling on foot has the ability to inspect areas of the facility, which otherwise may not be inspected routinely. This ability to easily conduct routine inspections is important for the detection of a hazardous situation which may be present at the site.

In addition, foot patrolling can be utilized as a great public relations tool, by placing Security Officers in direct contact with employees, visitors, and customers, assisting with security concerns and educating them regarding safety matters. So it's easy to see why foot patrols are such an intricate part of a comprehensive security program, because so many things can be accomplished through the use of them.

- **Vehicle Patrol**

The second most common method of patrol is the vehicle patrol. Patrol vehicles can come in many styles from the standard patrol car, to trucks, vans, utility vehicle, or golf carts. In addition, patrol vehicles may be equipped with standard, automatic, or four wheel drive transmissions. No matter what type of vehicle is utilized for the patrol operation, the purpose will usually be the same. Patrol vehicles are generally used for patrolling large outside areas of the protected site. Patrol vehicles allow the Security Officer to cover more outside area in the least amount of time. A Security Officer has the ability to respond faster to situations occurring within the area of patrol when a vehicle is used. Patrol vehicles can also have a great crime deterrent value associated with them because they are very visible to the public.

Areas of Patrol

Areas of patrol are divided into two basic categories, **Interior** and **Exterior**. Generally, Security Officers will conduct some form of interior or exterior patrols, or both, of the site in which they are assigned. Interior patrol can be defined as any patrol conducted inside a building or structure. Exterior patrol can be defined as any patrol conducted of the areas outside of a building or structure. The goal of patrolling interior or exterior areas is the same, protection and observation.

- **Interior Patrol**

In general, interior areas of a building will be the most important areas of the site to be patrolled. The largest percentage of your time on duty will be spent conducting patrols inside buildings. This is due to the fact that most of the critical operational functions of a business, as well as their most valuable assets, are maintained within the walls of their buildings. Because of this, interior security patrols are a key element of any loss prevention or security program and become an integral part of the daily routine of security personnel. Most interior patrols are performed on foot, generally because the inside of buildings cannot accommodate vehicle traffic, with the exception of golf carts in some situations. The following is a list of areas which may be included during a common interior building patrol:

- Office areas.
- Restrooms and break rooms.
- Supply or equipment storage rooms.
- Computer rooms.
- Entrance and exit areas.
- Doors and windows.
- Hallways and stairwells.
- Warehouse areas.
- Loading docks and shipping areas.
- Fire protection equipment.
- Maintenance areas or boiler rooms.

This is just a partial list of the areas which could be included in an interior patrol of a building. All businesses are slightly different. Each with its own emphasis on what should be considered important. Also, most buildings will be slightly different with regards to their size and design, which could have an impact on how patrols are conducted. But in general, most businesses which have established a security program will incorporate some form of systematic patrol into the planning, to insure that important areas are routinely being inspected.

- **Exterior Patrol**

Exterior patrols are conducted in the outside areas of a protected site. This type of patrol would include the grounds surrounding all buildings, parking lots, outside storage areas, and the perimeter of the facility. Exterior patrols are an important aspect of the overall protection program, because they are the type of patrol that is most visible to the general public. Exterior patrols should convey the message to anyone watching the property, that this site is protected. And hopefully this message will be enough to deter potential criminals from committing acts against the property. Since exterior patrols are conducted in outside areas, Security Officers may be exposed to additional risks, so officer safety issues must be stressed. Exterior patrols can be performed on foot, as well as in patrol vehicles.

Patrol Philosophy

There are two basic philosophies regarding the way in which security patrols are conducted. The first is called '**high visibility patrol**'. What the term implies is that a strong security presence is desirable on the property. Generally, Security Officers will conduct patrols in a very open manner, almost as if they were on display. The goal of high visibility patrol is to bring attention to the security program, by sending the message that security is taken seriously at the facility. There are numerous tactics which can be employed to accomplish this goal. For foot patrols, tactics may include Security Officers patrolling in pairs, several officers patrolling different areas of the facility at the same time, or overlapping security patrols. Security Officers will generally be required to dress in highly professional police style uniforms, and conduct an extensive public relations function.

For vehicle patrols, high visibility tactics may include highly visible security marking on patrol vehicles, conducting patrols with multiple vehicles, two officers assigned to a patrol vehicle, conducting patrols with flashing security lights, etc. No matter what tactics are applied, the message of a strong protective presence is the goal.

The second type of patrol philosophy is known as '**low visibility patrol**'. This type of patrol philosophy is utilized at facilities where the appearance of a strong security presence is not desired. This is not to imply that strong security is not wanted at facilities utilizing this philosophy, it implies that the facility may just not desire that appearance. We should always assume that companies have their best interest in mind when it comes to protection. Tactics which mark this type of philosophy include, Security Officers dressed in low profile uniforms such as suits or polo shirts. This type of dress is very well suited for corporate security or retail loss prevention operations. Security patrols may be kept to a minimum, and Security Officers may have little contact with personnel working at the facility. If vehicle patrols are conducted, they are usually performed in unmarked patrol vehicles or vehicles bearing only the logo of the business. Generally, facilities utilizing this type of patrol philosophy expect the protective function to be conducted in a 'low key' manner.

Conducting the Initial Patrol

Security Officers are commonly required to conduct multiple patrols during their daily tour of duty. While all patrols should be considered important, the first patrol conducted at the beginning of the shift must be considered extremely important. It's during this initial patrol that the Security Officer can assess the current situations and level of security which exists at the facility. It's unimportant how many patrols a security Officer has conducted at the facility in the past, situations often change quickly. It is important that the Security Officer have a basic knowledge of the current conditions at the facility immediately after he arrives on duty. Having this information enables the Security Officer to more easily detect abnormal situations as they occur, instead of being caught completely off guard. From a safety stand point, the initial patrol is important because it gives the Security Officer the information necessary to know where to place attention during subsequent patrols.

Fixed Post Assignments

A Security Officer will generally be assigned a fixed duty post during times when patrols are not being conducted. These fixed post assignments, and the procedures associated with them, can vary greatly from facility to facility. The Security Officer may find himself / herself posted at a gatehouse, in an office, at a reception desk, etc. We will not spend time exploring all the various fixed duty post assignments you may encounter during your career. However, we will examine the general philosophy of these assignments. It is also important to remember that no matter what type of fixed post assignment you find yourself assigned to, you should become familiar with all aspects of the post. Read all post orders and ask questions if necessary.

In the security industry the vast majority of fixed post assignments will fall into one of two categories; **Checkpoints** and **Surveillance Posts**. The following will provide you with a basic understanding of these two types of post assignments and the duties associated with them.

- **Checkpoints**

Checkpoints are post assignments where the Security Officer has direct control over the ingress /egress of people and vehicles through an area. These types of posts may be positioned at an entry or exit point, such as gates or doorways. Security Officers assigned to checkpoints routinely work at a gatehouse or reception desk. The duties at these checkpoints can include, but are not limited to:

- Identification checks.
- Issuing identification badges.
- Maintaining visitor sign-in registers.
- Verifying supply deliveries.
- Operating electronic access systems.
- Operating metal detectors or x-ray equipment.
- Physically searching personnel and their belongings.

Security Officers assigned to checkpoints must have a firm understanding that the goal of the operation is access control. If access control procedures are not an element of the operation, it's not a checkpoint. Written procedures should be established for all checkpoint operations. This will provide the Security Officer with the information necessary to perform his / her duties effectively.

- **Surveillance Post**

The second type of fixed post assignment is known as a 'surveillance post'. A surveillance post is generally an assignment where the Security Officer's primary duty is to observe and report. Access control is not an element of surveillance post assignments. Surveillance posts may be covert (hidden) or overt (open). A surveillance post may be part of a retail establishment's loss prevention program, in which shoppers and employees are monitored. A Security Officer may be assigned to a facility's lobby for the purpose of monitoring the activity of personnel in the area. This too is a surveillance post. Security Officers assigned to surveillance posts may be required to use or operate equipment such as cameras or binoculars. Another form of surveillance post is the security command center. This type of surveillance post generally includes the monitoring of facility wide Closed Circuit Television (CCTV), communications, and intrusion detection systems. So it really doesn't matter where the surveillance post is located, the primary purpose of the assignment will be observation.

Security Patrol Vehicle Maintenance

by

Nick LaFleur

Anyone who uses a vehicle to assist in either residential or citywide security patrol knows that one of the fundamentally priceless commodities they have is proper and safe operation of their vehicle. The most important aspect of that vehicle is the maintenance that is done to it on a regular basis. Security vehicles provide not only a visible and expedient way to conduct patrols, but can often times be the deciding factor in an officer safety and resolution to a security issue. Routine inspections of vehicles involved in patrols keeps the officer and those paying for the service safe and able to operate within the parameters of the specific function.

Inspections should occur once at the beginning of every shift or tour of duty. At minimum, they should be conducted once a week. Regular checks of tire pressure, fluid levels, hoses, brakes etc. can prevent costly repairs and down time for the vehicle. In situations where only one vehicle is available, these checks play an even greater role in the function and safety of patrolling. All officers should not only conduct the vehicle checks, but also become familiar with the aspects of vehicular maintenance and minor repair. Keeping maintenance logs of all items checked daily will assist managers and officers in preparing and using a well-rounded vehicle maintenance policy. Accountability is accomplished by requiring all officers to sign daily checklists as each item is inspected.

For overall maintenance and to keep the vehicle in good condition, choose a qualified service center to perform inspections on a routine basis. Becoming familiar with a service center can afford the company good relations and sometimes discounts on services. When choosing a service center, make sure the mechanics are ASE certified and have the qualifications necessary to perform various tasks on that particular vehicle. All reputable service centers will provide their qualifications when asked. It sometimes helps to choose a name brand or franchised service center that is found in other cities or states, should it become necessary to use the vehicle outside of the normal locale. Smaller service centers, such as those owned and operated locally, sometimes offer cheaper prices on services, and often employee technicians as qualified as their larger counterparts.

In this article we will explore the basic list of inspection areas and common problems found while operating patrol vehicles.

Exterior Lights

All external lights should be checked once per shift, even on patrols that only occur during daylight hours.

Check spotlights or bar lights if applicable, including take down lights, alley lights etc, in all combinations. If bar lights are used, make sure the electrical system can withstand the load. Normally, manufacturers will give recommendations on usage of bar and spot lights, but if this is not available, a low-cost meter from a local auto parts store can measure not only alternator output but load as well.

Make sure both headlights are functioning in both high and low beam modes.

Check turn indicator lights on the front and rear of the vehicle. Check parking and marker lights front and back. Make sure to carry at least one spare of each type of bulb that the vehicle uses. Brake lights should be checked as well by using another individual or if no one is available, using a flashlight or tire bar to depress the brake pedal while checking.

Interior Lights

Often overlooked, internal lights provide for the officer's safety and convenience. Make sure Check dome lights, courtesy lights and dashboard lights. Make sure all vital controls such as the speedometer and gear indicators as well as fluid and temperature gauges are fully lit up and working during operation. Dashboard lights on some vehicles can be costly to repair, but safety should never be hampered by cost.

Battery

Most late model batteries do not require the usual maintenance of their older counterparts. Filling the cells with water frequently shows a possible problem. It is still important, however to check the water level, for the sake of preventing drying out of the cells. It is recommended that the cells be filled up to the first part of the bottom of the filler hole. This will be a temporary fix until a new batter can be purchased. Check for corrosion around the battery terminals and wires. Corrosion, in the form of a yellowish-green residue, is also corrosive to skin and clothes, so use care in handling it. Temporary cleaning of corrosion can be accomplished by a light coating of soda, such as found in soft drinks. This neutralizes the corrosion, which then can be wiped away. Always keep terminals and wires clean and free of any debris, corrosion as well as dirt hinders the actual performance and life of a battery. When installing a new battery, apply a small amount of Vaseline to the terminals and terminal connectors. There is also an industry grade terminal coating that can be purchased from most auto parts stores to help prevent corrosion and thus increase the life and performance of the battery. Check for bulges, cracks, or dents as well as evidence of leakage from the battery. Any of the aforementioned indicators show that the battery is in trouble and should be replaced at the earliest opportunity. Never smoke near or around the engine or battery and related parts.

Brakes

Obviously a safety feature that must not be ignored, oftentimes attention is only paid to this feature when problems are evident. Simple checks can prevent high repair costs and save lives. Checking the brakes without taking the wheels off is possible, but for a full inspection, an authorized mechanic should perform this vital check. For general purposes, make sure that only minimal effort is required to bring the vehicle to a complete stop. Make sure the wheels do not lock up when normal stopping is attempted. The brake pedal should not feel spongy or make noises that resemble air being forced into or out of the system. The pedal should depress with an even resistance and should not go all the way to the floor. Visually check the inside and outside of the front rotors (this is where the wheel attaches onto the front axle) the rotors are the surface upon which the brakes make contact and stop the vehicle, so the surface should be relatively smooth and free of gouges or cuts. During normal wear, visible crevices appear in addition to large amounts of brake dust that show up as a dark powder on the outside of the wheel and around the rim. This is normal; however, make some effort in cleaning excess dust from the rotors and wheel to keep the dust from accumulating to an unmanageable point. Make sure there is no noise coming from the rotors. On many vehicles brake parts are equipped with wear indicators, which emit a high-pitched scraping sound when activated. The wear indicators are small pieces of metal that hide beneath the brake lining, when the lining is worn to the beginning of an unsafe level, the metal begins to slightly scrape, thus emitting the noise. This in itself is not dangerous, but should never be ignored because it is designed to warn the driver of impending brake problems. Check for leaks, or evidence of fluid around all lines near the brake calipers and rear drums. Calipers are the units that hold the brake pads which when applied to the rotor allow the vehicle to slow down and stop, they are located on the top of the rotor and appear as two metal blocks covering both the outer and inner rotor edge. The brake line is attached somewhere behind the top part of the caliper. Any evidence of fluid in the vicinity of the brake units and parts suggests a probable brake fluid leak, but could also point to an oil or transmission fluid leak. Fluid levels should be at the recommended settings, usually marked on the fluid reservoir in the engine compartment. Over filling any fluids in a car can be as bad as not having the proper amounts.

Shocks/Strut's and Suspension

For the proper performance of tires and the general safety of driving, shocks and struts are important to maintain, although not as frequently changed as other vital parts on a vehicle. These components of the suspension system keep tires on the road during normal as well as strained driving conditions such as rain or poor roads. The condition of these components can also increase the life of the tires. The general rule of thumb for testing shocks or struts is to push on the front or rear bumper as far down as it will allow, enough to cause the vehicle to bounce slightly. When released, the vehicle should bounce to a stable condition within three or fewer movements. Additionally, check the tires for worn patches in circular and sporadic patterns, this can indicate worn shocks. This is a general rule, and does not take the place of a qualified mechanic testing their condition. Checking for leaks or wetness around the shock or strut housings is also a sign that the shocks or struts may have damage and should be replaced. Quite a few auto parts stores sell shocks and struts with a limited lifetime warranty, making the initial purchase the only expense involved, other than the labor to install the shocks or struts. This is a less expensive means than buying new parts each time. Most service centers will install parts other than their own, some do not, so make sure to check with them first.

Tires

Along with the suspension system, tires effectively assist in the safety and performance of the vehicle. Fuel economy as well as ride comfort is affected by the condition of the tires. Most tires have wear indicators built into the tire rubber. Along the tire tread, these indicators show a path across the tire tread, slightly higher than the absolute base of the rubber. When viewing a normal tread pattern, you see the grooves between the tread, when the groove wears down to the indicators, there is a smooth bridge that is formed from ridge to ridge, this is the time to think about replacing tires, as any more wear could prove dangerous and costly. Tire tread channels water and other road debris away from the driving surface of the tire and promotes traction. Bald tires, or tires whose tread has been depleted can lose control on slippery surfaces and cause injury or even death. In some situations it is noticed that security vehicles are driven at constant slow speeds, with hard turns made in either direction, thereby causing slightly more wear to the outside edges of the front tires. This can be dealt with on some levels by making sure the vehicle is always aligned properly, and the tire pressure is within specifications. All vehicles should have a tire pressure gauge handy, and the pressure should be checked each time the vehicle is fueled or serviced. Additionally, some vehicles can have their alignment set in such a way as to provide better wear for the specific driving condition. Avoid buying used tires or having different brands of tires on the same axle. Currently there are many different tire manufacturers that offer low priced, high wear tires for all applications. The life expectancy of a tire is measured by the code that is stamped on the tire an authorized tire dealer can provide more information on the specifics. Things to make sure about when ordering new tires is that they are sufficient for the load the vehicle will carry, adequate for the climate and road conditions (a good all season tire is usually sufficient). All vehicles should have a spare tire that is rated for that vehicle. A full size spare (regular tire) is optimal, but in some cases is impractical and therefore a standard spare or "donut" is used. Make sure the vehicle has a tire jack and lug wrench specifically designed for that vehicle. Changing tires should be done on a flat, even surface as far from the roadway as practical. Using flares or traffic cones to draw attention to the vehicle is a safe way of avoiding unnecessary risk. Checking the spare tire should become a habitual part of the overall maintenance check. NOTE: Tires that are not used will deflate incrementally and therefore should be checked for pressure at the same intervals as the tires in use.

Oil

The lifeblood of the vehicle, this is one of the most ignored fluids and the most important for the life of the engine. Oil prevents friction within the engine from destroying valuable components and keeps the engine running at moderate temperatures during all climates. Oil checks should be conducted at every shift change or tour of duty. Checking the oil should be done after the engine has been brought to operating temperature, as indicated by the dashboard temperature gauge, or for at least five minutes of running or idle time if no gauge is present. Oil is checked via the dipstick, the thin metals stick that is located in the engine compartment and often has a looped handle at the end. The car should be warmed up and engine NOT running to properly check the oil in most cars. Refer to the vehicle's instruction manual to learn about specific methods for the type of vehicle you are using. The stick should be pulled out and wiped clean, then inserted fully and once more pulled out. The level is normally shown by a thatched area somewhere near the bottom of the dipstick, normal levels show oil between two arrows marked "normal" or "full" but this can vary from vehicle to vehicle as well.

Never run the engine with low oil, or with the oil warning light on. Take care to not overfill the oil. Add half a quart of oil at a time, let it sit or run the engine for about a minute, then repeat the check process until the oil is within specified levels. Recheck within three days to make sure the low oil is not caused by a leak or abnormal processes. The type of oil to use depends upon the climate, driving conditions and engine type. Refer to the vehicle's user manual for suggestions. Engine oil should be changed, including the filter, at least every 3000 miles. Refer your vehicle to an authorized service center for this procedure.

Transmission Fluid

Checking transmission fluid does not have to occur with the same frequency as other fluids, but within the operations of a patrol vehicle, should still be checked at least once a month, more if driving conditions such as use in dusty or off-road areas, working under heavy load, frequent starting and stopping, or abrupt acceleration/deceleration are present. Low fluid in the transmission can be marked by a grinding or medium pitched scraping noise coming from the center of the vehicle but may project the noise to anywhere in the undercarriage. Slipping of the gears can occur when the vehicle accelerates, and in developed cases, even when the vehicle takes off normally. Difficulty in shifting in both manual and automatic transmissions is also a possible indicator of low fluid. Any warning from the transmission should never go unchecked. Generally, transmission fluid in an automatic vehicle should be checked with the engine running, in park, and warmed up. The method is the same as for checking engine oil. Using the dipstick, wipe it and reinsert it, then check the level as marked by the indicators on the bottom end of the stick. Remember to not overfill. Automatic transmissions have screens and filters located in the transmission and should be serviced at least once a year, more if heavy driving conditions exist. This action should be performed by an authorized service center so as too not affect warranties.

Manual transmissions differ slightly; there is usually no dipstick for checking in the engine compartment. Generally, most manual transmissions are checked at the transmission housing under the vehicle. For the proper check it is recommended that an authorized service center perform the inspection. Filling low fluid in a manual transmission sometimes requires the use of small fluid dispensers and may involve jacking or hoisting the vehicle first. It is for this and other reasons, such as ease of patrol in low speed situations, that automatic transmissions provide much easier use and maintenance.

Fuel

Normally, any grade of fuel is sufficient. Octane ratings, used to denote different grades of gasoline, are recommended by the vehicle manufacturer and are generally talked about in terms of performance enhancements. The average patrol vehicle would easily run on the lowest grade (currently 87 octane) but for higher efficiency and cleaner burn, at least 89 is recommended. High performance vehicles that may engage in rougher acceleration and longer overall trips might wish to use the highest rating (currently 93-95 depending on location). Contrary to popular belief, certain vehicles do run better on different brands of gasoline, even though all gasoline is essentially the same, except for the individual company processing methods and additives. What may work wonders in one vehicle, may in fact be less effective in others. Generally, however, fuel will not be a problem. Make sure that vehicles are used regularly to avoid the gasoline sitting in the tank for too long, as this can cause problems due to condensation and break down. This is sometimes the case in fleet vehicles that sit for long periods of time between uses.

Windows

A commonly disregarded component of the vehicle, windows and windshields are taken for granted as long as they are not broken. It should be noted, however, that a dirty or grimy window can pose a safety risk in much the same way as a cracked or broken glass. Smoking can coat the interior glass with a film sufficient to prevent a clear view, especially at night. General use also allows normal dust and dirt to adhere to the interior glass surfaces thereby decreasing visibility. In wet conditions, dirty interior glass can fog up that much easier. Cleaning the interior glass should be as important as the exterior glass and should not be overlooked in the overall vehicle maintenance plan. Use of common window solutions that prevent fogging or that assist in rain runoff are sometimes helpful, but operators should take care to read the instructions fully and make a decision on the usefulness based on their individual needs and operating conditions.

Fuses

Inspecting interior fuses can prevent costly or dangerous system failures. Locating the fuse box is done via the vehicle manual, but most often will be located under the dash on one side of the vehicle. Inspecting fuses for cracking, burns or lose fits is simple and takes no more than 3-5 minutes. Visually inspect the fuse itself for cracks, tears, darkened burned plastic or for the actual separation of the filament used inside. Inspect the fuse socket for breaks and burn discolorations. This simple inspection can prevent a blown fuse during an inopportune time, and can also be the first step in fixing a vehicle problem prior to having maintenance performed. Checking fuse condition should be the first step in diagnosing of failed components such as interior power adapters/lighters, lights, indicator signals, radio etc.

Door locks

Another overlooked component of the vehicle, door locks can provide instant safety to an officer or passenger and should be in full operating condition. Manual locks are more dependable, but require slightly more effort in terms of time. Automatic locks which can afford the officer a complete lock down of the entire vehicle are convenient, but offer more parts that may need replacement, which can oftentimes be costly.

You have seen some of the integral parts of a vehicle and their operating guidelines. Always give a patrol vehicle the high regard and respect it deserves when maintaining and using it. Safety, comfort and convenience are traits that can be enhanced by regular inspections. High cost repairs and danger to life and property are consequences of poorly maintained vehicles. Remember that all vehicles are inherently different and use care when changing from a familiar vehicle to an unfamiliar one. Get used to the acceleration and breaking features, as well as the normal operating functions of any vehicle you are in possession of. As a manager, make sure all those charged with the responsibility of using and maintaining the vehicles are fully trained and have the equipment and knowledge to carry out their specific functions. Checklists and other forms of accountability should be used to keep vehicles are officers working at the highest level of safety and professionalism.

Safety at Automated Bank Teller Machines (ATM's)

by

Wade M. Knapp, CPS

Automated Bank Teller Machines (ATM) provide us with a convenient source of 24 hour a day banking. While the vast majority of daily ATM users experience no problems during their transactions, some safety risks have been associated with the use of these bank teller machines. The primary safety risk associated with ATM use is the crime of robbery, however other crimes such as abduction, sexual assault, and vehicle theft have been reported as well. Over the years, financial institutions have greatly improved safety measures at these machines through the application of video surveillance and security lighting, along with selecting machine locations which provide for improved observation. What should always be remembered is that while physical and technical security measures do improve safety, their application alone can not guarantee that a crime will not occur. We must also develop and employ personal safety procedures when using our ATM's if we truly wish to reduce our crime risk exposure. The following basic safety precautions should be considered and applied in order to make your ATM transactions as safe as possible.

- If possible, refrain from using ATM machines during late night hours.
- Avoid using ATM's which are located in secluded areas or ATM's which cannot be seen from the street.
- Whenever possible, use ATM's which are located in well lighted areas where other people are present. Today many ATM machines are located within retail businesses, adding an extra degree of safety for the user.
- Use drive-up ATM's when possible. Remember to keep all vehicle doors locked.
- If using a walk-up ATM, park as close to the machine as possible.
- Observe all surrounding areas before approaching the ATM machine.
- If someone else is using the ATM machine, wait in your vehicle until that person is finished with their transaction and leaves.
- When using the ATM, complete your transaction as quickly as possible. Attempt to limit transaction times to under a minute.
- Be aware of your surrounding while conducting your transaction. Be observant.
- Never allow another person to approach within arms distance while you are completing your transaction. Be firm, tell the person to step back and remain at a safe distance.
- When you complete your transaction, quickly return to your vehicle and leave the area.
- Remember to take your transaction receipts with you. These receipts contain personal information regarding your account, so leave nothing behind at the machine.
- If you are approached be someone with a weapon demanding your money, remain calm and give them the money, your personal safety is more important.
- If you are the victim of a crime or witness a crime at an ATM machine, notify the police immediately with the details of the crime.

Safety Precautions While Staying At Hotels or Motels

by

Wade M. Knapp, CPS

Anyone who travels is accustom to spending time in hotels or motels. Lodging establishments can range from the large multi-level hotels to the small family owned bed & breakfast. While these lodging establishments can vary greatly in both style and cost, there are certain elements of risk associated with any of them. Unlike your personal residence, hotel management controls and provides for your safety and protection during the stay in their establishment. We as guest assume that the establishment has the upmost concern for our personal safety, and more than likely this statement is true. However, is concern enough? Does the establishment truly have an understanding of safety risk management and are precautions being taken? Consider a hotel which has hundreds of guest rooms, but only two employees on duty during the night shift. Unless access control procedures and surveillance technologies are applied throughout the facility there is no way to monitor or control who is moving about the establishment. Is the person walking up the hall at 1am a guest returning to their room or a criminal who just walked in off the streets? Add to this, the risk associated with fires, medical emergencies, vehicle security, etc. and its easy to see why one should consider their personal safety and take precautions. The following are some basic safety precautions you may want to think about before your next stay in a hotel or motel.

- Always select a reputable, well maintained hotel or motel.
- Whenever possible make reservations in advance to insure that a room is available.
- Don’t select a hotel or motel which is located in a secluded area of the city.
- Consider selecting hotel or motels which have security personnel.
- If possible, select an establishment that utilizes card-key access on guest rooms.
- Beyond the lobby, are entrances to the establishment accessible only through the use of guest room keys, or are they open to the general public?
- Obtain clear, exact directions for the location of the hotel or motel.
- Consider not excepting rooms in secluded areas of single story motels.
- Always note the location of emergency exits and elevators. Know how to evacuate in the event of an emergency.
- Note the location of fire alarms and fire extinguishers on your floor.
- Be cautious when using stairways.
- When returning to a hotel during night time hours refrain from using side entrances, always enter through the lobby.
- Remember your vehicle and parking safety precautions.
- After checking into your room, test all door and window locks to insure they are working properly.
- Make sure the telephone is working properly and a telephone directory is present.
- Check all areas of the room, including under the bed, for suspicious or hazardous items.
- If you discover that something in the room is not working properly, or you discover something suspicious, report it to the hotel office and ask to be moved to another room.
- Keep doors and windows locked while in or out of the room.
- Close window blinds before unpacking your luggage.
- Consider the use of a portable smoke detector for added fire safety.
- Consider the use of a portable door alarm for added security.

- If someone knocks on the door, know who it is before opening the door. Ask for identification and verify it with the hotel office.
- Don't accept mail or packages which have been sent to the room or left at the door. Verify the sender of all deliveries with the hotel office prior to accepting them.
- Keep a flashlight in the room.
- If you are traveling with a cellular telephone, keep it with you while in your room.
- When traveling with children, never leave them alone in the hotel room.
- Don't allow small children to answer the door.
- Leave a light and the television on when away from the room.
- Consider securing valuables in the hotel safe, or room safe, if this service is available.
- Consider tipping the housekeeping staff.
- Don't conduct business activities in open public areas of lobbies or lounges.
- Don't discuss personal information or travel plans with strangers you meet in the hotel.
- Don't invite strangers to your room.
- Insure that you have your room key prior to leaving the room.
- Report all suspicious activities to the hotel management or security.
- If you detect something suspicious upon returning to your room, do not enter the room. Go to the lobby and report it to hotel management.

Protection Officers and the Press

by

Wade M. Knapp, CPS

The first step in developing an effective relationship with members of the news media is understanding the function of the press. Simply put, the press has the job of reporting the news to the public. Today the news is a 24 hour a day, globally reaching business that encompasses television, radio, newspapers and magazines. National and International news agencies, their reporters and cameramen are constantly searching for stories that may interest and inform the general public. From the city streets in the United States to a battle field abroad, the members of the press often times risk their own lives to report these stories. In addition, with the advances in technology, news reporting has become nearly instantaneous, allowing the general public to watch these stories as they unfold. The combination of dedicated news professionals and advanced news reporting technologies can nearly guarantee an important news story is never out of reach of the camera's eye.

Incidents involving violence, crime or terrorism are usually considered important news stories and generally end up as headlines in all forms of the press. If such an incident were to occur you can be assured that news media resources would be mobilized to cover the story. It should also be easy to assume that news agencies would attempt to report such a story in as extensive detail as possible. This detailed coverage of the event could include; live reporting from the scene of the incident, interviews with Law Enforcement, Fire Department, EMS officials, company management, incident victims and their families, etc. With this reality in mind, it is necessary to conduct advance planning in the area of news media relations in order to be prepared to effectively handle such an event.

All companies should have established policies and procedures for handling a news media event. These policies and procedures should be implemented to insure that key areas of importance such as; personnel safety, operational security, and proper information dissemination are addressed. The following are key points to consider when developing policies and procedures for handling news media events:

> Policies and procedures regarding the news media should be developed to insure proper handling of press matters during an event, as well as non-event times.
>
> All polices regarding the dissemination of information to the press should be in writing.
>
> During an actual incident Security Officers should refrain from granting press interviews. During an event, Security Officers will most likely be busy with the task at hand, unnecessary distractions should be kept to a minimum. Request for information by media personnel should be referred to the company Public Information Officer or the Information Officer operating through the Incident Command System (ICS). This should insure the continuity of information dissemination throughout the event.
>
> Consideration should be given to creating policies and procedures for handling request and/or attempts by news media personnel to gain access to protected areas of the site.

Staging areas for news media crews must be established in advance. Consideration should be given to insuring that press personnel have the space necessary to operate without interfering with medical operations.

It should be remembered that press officials are not granted any special authority or rights to enter on private property, remain on private property or force persons to make statements. If press officials have enter into an area where their presence is not authorized, simply refer them to the Public Information Officer and ask them to leave. If they do not honor the request, notify local Law Enforcement for assistance.

Security Officers should refrain from engaging in any altercations with press personnel. Never threaten, push or strike a member of the press. Never place your hand over the lense of a news camera, grab a news camera, etc.. If you do not want to make a statement at that time, simply don’t.

FIRST AID BASICS

by

Lee A. Knapp, RN, CEN

First Aid is defined by the Webster's dictionary as emergency care or treatment given to an ill or injured person before regular medical aid can be obtained. At any time, you may be confronted with a medical emergency in which you will need to administer first aid.

Medical emergencies come in all shapes and sizes, from a minor cut or scrape to a heart attack or stroke. Your ability to recognize such emergencies and respond quickly and appropriately may mean the difference between life and death. The following information is designed to enable you to recognize such emergencies, call for Emergency Medical Services (EMS), and administer basic first aid techniques until help arrives. Remember, first aid **is not a substitute for professional medical treatment**. The information presented in this document reflects only basic first aid techniques. It should not be utilized as a substitute for professional CPR and First Aid training. It is strongly suggested that proper training in CPR and First Aid be obtained. For information regarding CPR and First Aid training, contact your local chapters of the American Red Cross or American Heart Association, or contact us at Protective Research Group, Inc.

Notifying Emergency Medical Services (EMS)

In any situation you may be confronted with, your first action should be assessment, or observation of the scene. At that time you will be able to determine if a call for help is necessary. Calling for help may include yelling for someone across the street or calling **911** by telephone. If you're obtaining assistance from another individual, always tell the person what you have observed, the location of the emergency, and tell them to call **911**. An example of this would be, "**I need help. There is a man unconscious in the parking lot, middle of the 2nd row. He is not breathing. Call 911**." If you are notifying Emergency Medical Services yourself, remember to remain calm, give your name, the location of the emergency, the type of emergency, and be as detailed as possible. At this time you will begin to render basic first aid to the person in need.

Assessment And Information Gathering

When rendering first aid to a person in need, a systematic approach is necessary to assess the situation, gather information and begin assistance quickly. This can be accomplished by following these steps:

- Scene survey
- Primary survey
- Secondary survey
- Environmental survey
- Patient history of illness / injury
- Witnesses to the event

- **Scene Survey**

Upon finding an unconscious or injured person, an observation of the scene must be made for safety prior to your attempting to assist this person. You must ask yourself "if I were to enter into that area, am I at risk of being injured myself?". Observing the scene for possible risks such as downed powerlines, falling objects, a growling dog, etc. could injure you and make you a victim as well, therefor not helping the already unconscious or injured person. In these such instances, calling 911 and relaying your observations of unsafe scene conditions is important for rescue workers so that they will arrive with the proper equipment and/or personnel needed to make a safe rescue.

- **Primary Survey**

The primary survey is conducted by assessing the **ABC**'s upon first encountering the ill or injured person. The **ABC**'s are defined as **AIRWAY, BREATHING, and CIRCULATION**. Each is surveyed in this order. Without an open airway, a person can not breathe. Simply by opening the airway, respirations may be restored without further intervention. If the person still does not breath, breathing must be done for the person. Finally, circulation must be assessed. This is done by feeling for a pulse at the carotid artery in the neck. If a pulse is felt and breathing has not been established, then rescue breathing is all that is necessary. However, if no pulse is felt, then CPR must be initiated.

- **Secondary Survey**

The secondary survey consists of assessing for and treating other life threatening emergencies. At this time you are looking for possible reasons as to why the person is ill or injured. Examples could be: profuse bleeding from an amputated limb which has rendered the person unconscious, a broken or deformed limb, a gunshot wound which is bleeding, etc. While conducting your secondary survey, this is the time in which you will control bleeding, apply splints to deformed limbs, taking other actions as necessary, and making the person as comfortable as possible until help arrives.

- **Environmental Survey**

The environmental survey consists of examining the area to gather information which might be vital to the care of the ill or injured person. Was the person working on a ladder and fell? Was the person working with electrical equipment that could have caused electrocution? Is the person's amputated finger within sight? This type of information must be collected and reported to EMS personnel.

- **History Of Illness / Injury**

Obtaining information about the person may be found by looking for medical alert bracelets and necklaces, identifying information in the person's wallet or purse, or by family members present at the scene. This information is useful in the treatment of the person and should be given to EMS personnel.

- **Witnesses To The Event**

Additional information should be gathered from witnesses to the event. Valuable information can be gathered as to what the person said, how the person was acting, and the exact nature of the illness or injury's occurrence can be identified. This information should as well be passed on to EMS personnel.

Cardiopulmonary Resuscitation (CPR)

Cardiopulmonary Resuscitation (CPR) is done when a person is absent of breathing and heartbeat. It is a way to help restore circulation of oxygen carrying blood to vital organs of the body. By breathing into the person's lungs, you are placing oxygen in the body. By performing chest compressions, you are circulating the blood to pick up the oxygen in the lungs and carry it throughout the body. CPR that is performed properly and promptly can give victims the time to receive treatment by advanced medical techniques. It is advised by The American Heart Association and The American Red Cross that all people should be trained in CPR.

Rescue Breathing

In finding an unconscious victim, you should shake and shout to the victim to determine responsiveness. If no response is obtained from the victim, you should call for help immediately. This may mean leaving the victim for a short period of time. Do this as quickly as possible. Upon returning to the victim, determine unresponsiveness again, by shaking and shouting. If the victim still does not respond, carefully roll the person onto their back and kneel beside the person's head and shoulders. Open the person's airway by tilting the head back. This is easily done by applying pressure on the forehead with one hand and lifting the chin with the other hand. Now look, listen and feel for breathing for about 5 seconds. Do you see the chest rise? Do you hear the breathing? Do you feel the person's breath on your cheek? If the person is breathing maintaining the open airway is all that is necessary. If not, you must breathe for the person.

1. With the person's head in the tilted position.
2. First, pinch the person's nose with your finger and thumb.
3. Next, cover the person's mouth with your mouth making a tight seal so that air does not escape.
4. Blow a breath into the person's lungs and then uncover the mouth to allow the breath to be exhaled.
5. Repeat the procedure a second time.

Now you must check for a pulse. A pulse is most easily found in an adult or child at the carotid artery at the side of the neck. Place your fingers on the person's Adams Apple and slide your fingers toward you to the groove at the side of the neck. Check for the pulse from 5 to 10 seconds. If a pulse is present, continue rescue breathing only until the person begins breathing on their own or EMS arrives.

CPR - Adult only

If the person does not have a pulse, then a combination of rescue breathing and chest compressions must be administered. To perform CPR, position yourself in a kneeling position at the persons shoulders so that you can give rescue breaths and do compressions without having to move. To find proper hand position, locate the bottom of the person's rib cage that is closest to you. Using the hand that is closest to the victim's feet, place your first two fingers (index and middle finger) at the bottom of the rib cage and slide them along the rib cage border until you reach the breastbone (sternum). Locate the sternal notch and place these two fingers over the end of the sternum, called the Xyphoid process. Next, place the heel of your other hand on the lower part of the sternum next to your two fingers. Place your other hand on top of this hand and interlock your fingers. Now, rise up onto your knees with your shoulders up over the victim's chest. Compress downward approximately 1 ½ inches to 2 inches by using the weight of your body and not just your arms, for a cycle of 15 times at a rate of/or greater than 1 compression per second. Give two slow breaths as explained before (in the rescue breathing section) and repeat another cycle of 15 compressions.

Continue this series for approximately one minute and then check the victim for a pulse. If a pulse is present, you will no longer give compressions but may need to continue rescue breathing if the victim does not start breathing again. Monitor the person frequently for a continued pulse. If the victim does not have a pulse, continue CPR compressions and breaths and check again every 3 to 4 minutes for a pulse. Continue CPR efforts until: (1) another trained person takes over CPR for you, (2) EMS personnel arrive and take over care of the victim, (3) you are exhausted and unable to continue, (4) the scene becomes unsafe.

Common Emergencies

Heart Attack

Heart attack, also known as a myocardial infarction or MI, occurs when an artery of the heart becomes blocked, stopping blood flow to certain areas of the heart. Symptoms of a heart attack vary from individual to individual, but most commonly seen symptoms are: chest pain, sometimes described as a heaviness or as an indigestion feeling. Some people may tell you they feel like they have an elephant sitting on their chest. The pain can also radiate into the jaw or left shoulder and arm. Pain between the shoulder blades may also occur. These people also feel short of breath and are usually diaphoretic, or sweaty. Some people also may have nausea and vomiting. What you must do is make the person comfortable. Have the person lie down and loosen all restrictive clothing such as shirt collars and belts. Call 911 for EMS assistance. Do not give the person anything to eat or drink. Stay with the person until help arrives. Continue to assess the person and be ready to perform CPR if the person should become unconscious and have an absence of breathing and heartbeat.

Stroke

Stroke, also known as a cerebral vascular accident or CVA, occurs when an artery in the brain becomes blocked, stopping blood flow to certain areas of the brain. Symptoms of a stroke are also widely varied, but the most commonly seen symptoms are: slurred speech, drooping of one side of the face, staggering walk, weakness or inability to move one side of the body. You must also make this person comfortable by lying them down and loosening restrictive clothing. Do not give these people anything to eat or drink because some stroke victims are also unable to swallow. Call 911 for EMS assistance immediately. Stay with this person as well and assess the ABC's.

Shock

Shock occurs when there is insufficient blood returning to the heart for normal function. Shock can have many different causes such as large volume of blood loss, infection, drug reaction, trauma, poisoning, heart attack and dehydration. Symptoms of shock include paleness of the skin, a bluish or grayish coloring of the lips and fingernails, the face may be pinched and without expression, there may be a staring of the eyes, breathing may be rapid and shallow, occasionally there may be restlessness or excitement, and often the person may complain of extreme thirst. You must keep the person lying down with their head positioned lower than their feet. You can elevate their feet on a stool or chair. Loosen any tight clothing. Keep the person comfortably warm but do not apply heat. Avoid any unnecessary noise or questions and avoid moving person if at all possible. You may give only sips of fluids, but avoid it if possible, and do not give the person anything to eat. Control any bleeding that may be occurring. Call 911 for EMS assistance and continue to observe the person closely.

Seizure

Seizures are caused by over activity of the brain cells. People who have the disease known as Epilepsy have seizures, but there are many other causes of seizures other than Epilepsy. There are also many different types of seizures, but the ones that are the most frightening to people are called grand mal seizures. A grand mal seizure consists of sudden unconsciousness followed by successive contractions and relaxation movements of the arms and legs. Muscles of the head and face jerk. Bladder control may be lost during a seizure. Breathing stops and there may be frothing from the mouth. These seizures are short in duration and breathing should resume after the seizure is over. Some people may remain unconscious for a few more minutes, and some people may appear exhausted, weak, and confused. They will not recall the seizure. What you must do while witnessing a seizure is move any objects from around the person that they could become injured by. Do not attempt to force the persons mouth open during a seizure and certainly do not put your fingers in their mouth in attempts to keep their airway open. Call 911 immediately for EMS assistance. Once the seizure has stopped, do your ABC's assessment and maintain an open airway until help arrives.

Spinal Injuries

Spinal injuries can occur from anything that causes a blow to the spine. This can be caused by a fall, being struck by a car, etc. Spinal injuries that also injure the spinal chord can cause paralysis of the body. Spinal chord injuries stop necessary signals from the brain from reaching their intended destination in other parts of the body. Depending upon where the injury has occurred, the paralysis could be below the waist or the injury could have occurred in the neck causing paralysis from the chest down and causing the person to stop breathing. When confronted with someone having a possible spinal injury your first action is to make sure that the person is kept lying flat and does not move a muscle. Any movement of the body can cause broken spinal bones to injure the spinal chord. Call 911 for EMS assistance if you are in reach of a telephone. If not, stay with this person until help arrives and 911 can be called. Someone who is thought to have a spinal injury and is conscious or confused may attempt to get up while you are away calling for help so it is important to remain with them.

Continue to assess your ABC's and maintain firm stabilization of the person's head and neck until EMS assistance arrives. This can be accomplished by reassuring the injured person and having them remain calm and motionless. Should the person stop breathing at any time, you will have to maintain an open airway, **but now this can not be done with the head-tilt / chin-lift as you have learned earlier.** Any tilting of the head will cause movement of the cervical spine and possibly cause further injury. At this time you will do what is called a jaw thrust maneuver. Position yourself on your knees above the person's head. By placing your hands on each side of the person's face and lying your thumbs on the their cheeks with your thumbnails pointing toward their feet, hook your index fingers under the rear notch of the jaws under each ear and push the jaw upward toward the ceiling. This will bring the tongue forward so that the airway is not obstructed. Maintain this open airway until help arrives. Should you need to give rescue breathing, you will now have to cover both the nose and mouth, if the person is small, or close the mouth tightly and ventilate through the person's nose.

Head Injuries

Head injuries can occur anytime that a person has been struck in the head or has fallen and hit their head. Symptoms of head injuries can include unconsciousness, confusion, slurred speech, headache, nausea and vomiting, one pupil larger than the other. You must keep the person lying still and call for assistance from

EMS. Also remember that any injury caused to the head can also have caused injury to the spine. Stabilization of the head and neck should also be done until help arrives.

Impaled Or Imbedded Objects

Never attempt to remove impaled or imbedded objects. Always stabilize the object and await EMS's arrival. You may need to control bleeding as necessary.

Loss Of A Body Part

Loss of a body part can occur many different ways. It could be the loss of a finger(s), hand, arm, foot, or leg. The most important thing you need to do is control bleeding. By applying pressure to the injury or above the injury, blood flow can be slowed to the injured part of the body. For example, if a person has lost the tip of their finger in a machinery accident, by applying a clean, snug fitting bandage to the finger and hand and elevating the hand above the level of the heart, bleeding can be slowed until help arrives. If for instances the hand has been severed from the body and blood from the arteries is spraying, applying pressure to the wound directly, elevating the hand above the level of the heart and applying pressure to the artery above the wound by squeezing it against the bone, should help decrease the flow of blood. By squeezing the upper arm, with your fingers over the inside of the arm where the brachial pulse is found, or by applying pressure at the groin of a leg that has bleeding, bleeding can be slowed. If bleeding has not slowed, placing a tourniquet, as a last resort, made with a belt or piece of fabric applied tightly around the affected limb as close to the wound as possible can slow the bleeding until EMS arrives. Attempt to keep the person lying or sitting still until help arrives. Assess for signs of shock. Recover any body parts and give these to EMS personnel upon their arrival.

Choking

The universal symbol of choking is the person's hands around the neck or throat. Anytime someone is choking, observe them closely. As long as the person is able to cough in attempts to remove the foreign object, allow them to do so. But when the person is no longer able to talk or cough, or you hear a high pitched sound when they are attempting to breath, it is time to take action. As long as the person is conscious and standing, you will need to perform the Heimlich maneuver. This is done by standing behind the victim and wrapping your arms around the person's waist. Make a fist with one hand. Place the thumb side of the fist against the person's abdomen, in the midline slightly above the navel and well below the end of the sternum. Grasp the fist with the other hand. Press the fist into the person's abdomen with a quick upward thrust. Each new thrust should be a separate and distinct attempt to dislodge the foreign object. Continue this action until the object has been expelled or the person becomes unconscious.

If the person becomes unconscious, lie the person down on their back with their face up. Straddle the person's thighs and place the heel of one hand against the person's abdomen, in the midline slightly above the navel and well below the end of the sternum. Place the second hand directly on top of the first. You then must press into the abdomen with a quick upward thrust. Continue this action until the foreign object has been removed. Check the person's mouth frequently to see if the object has been forced into the person's mouth. Do this by performing a finger sweep from one side of the mouth to the other. If the person is not breathing, attempt Rescue Breathing. If you can not get air into the lungs, continue the abdominal thrusts and repeat finger sweeps and attempts at Rescue Breathing (as described earlier) until EMS personnel arrive.

In certain cases such as advanced pregnancy, abdominal thrusts can not be used. At this time, chest thrusts are done by encircling the person under the arms and placing the thumb side of the fist on the middle of the breast bone, taking care to avoid the end of the breastbone or sternum. You will then grab the fist with the other hand and perform backward thrusts until the foreign object is expelled or the person becomes unconscious. At that time, lie the person down as before and kneel beside the person's chest. Place the hands the same as you would to perform CPR. Each thrust should be delivered distinctly, and with the intent of dislodging the obstruction.

Fainting

Fainting, or syncope, is a loss in consciousness caused by inadequate blood flow to the brain. It can be caused by many different things, but usually does not last long and the person does not stop breathing. Causes of fainting can be due to illness, sudden changes in body position, unnerving sights such as seeing blood, etc. If the person is seated, place their head between their knees or lie them down. This promotes adequate circulation to return to the brain. Remove tight clothing. You can also place a cold wet towel overs the person's forehead until they regain consciousness. Call EMS for assistance.

Heat Exhaustion

Heat exhaustion is an acute reaction to heat exposure. Symptoms include weakness, dizziness, nausea, headache, and finally collapse. The person's face is pale, cool, and moist. The skin is cool, clammy, with profuse sweating. You should move the person to a cool place, loosen clothing, and lie them down. Keep them warm to prevent the onset of shock. Give fruit juices or sports drinks in abundant amounts. Call 911 for EMS assistance.

Heat Stroke

Heat stroke is an acute and dangerous reaction to heat exposure. It's symptoms vary from heat exhaustion in that the face is red, dry, and hot. The skin is hot, dry, and there is no sweating. The body's temperature is high, between 106 and 110 degrees. You must remove as much clothing as possible, except for undergarments. Keep the person at absolute rest with the head elevated. Without delay, apply cold packs or cold water to the person's body, direct a fan to blow on the person or turn air conditioning on high to help cool the person's body temperature. Call 911 for EMS assistance.

Splinting Of Limbs

An injury that occurs to the arms and legs can cause pain, swelling, and deformities of the bones due to fractures. The injuries need to be immobilized until EMS personnel arrive. This can be accomplished by splinting the injured limb. To splint an injury, you can use anything available to tie around the limb and keep it from moving. Examples of things that can be used as splints are sticks, magazines, pillows, etc.. The basic protocol for applying splints is as follows: to splint an injured bone, immobilize the joint above and below the injury. An example of splinting a broken forearm would be to place a stick along the arm from the below wrist to above the elbow and tying it in place at the top, bottom, and middle sections of the splint. To splint an injured joint, immobilize the bones above and below the injury. With some injuries such as shoulder injuries, you can place a belt or tie a piece of material around the upper arm of the affected body side and around the chest to keep the arm against the body, therefore preventing movement of the arm and shoulder. If one leg is injured, by splinting it to the other leg, this will prevent movement and possible further injury until help arrives.

HIV / AIDS Precautions

Acquired Immune Deficiency Syndrome, or AIDS, is a disease that alters the immune system, leaving a person vulnerable to life-threatening illnesses. Because of the depression of the immune system, the body is unable to fight off infections and diseases. AIDS is caused by the HIV virus, or Human Immunodeficiency Virus. It affects many adults in their productive years and most people have died within 5-10 years of being diagnosed with AIDS.

The HIV virus can be found in blood, body fluids, and tissues. Body fluids such as urine, feces, saliva, tears, and nasal secretions may contain small amounts of the virus. However, transmission of HIV has not been documented through any of these fluids. The sources of body fluids which contain large enough amounts of the virus and could transmit the infection are: blood, body fluids with blood, and semen and vaginal secretions. The HIV virus has been known to be transmitted through various ways such as sexual contact with infected persons, sharing of contaminated needles, blood transfusions before 1985, mother to baby, and exposure of cuts or broken skin to infected fluids. **The HIV virus is not spread by casual contact**. Casual contact is contact that does not involve the exchange of body fluids and include hugging, casual kissing, handshakes, or touching objects handled by an HIV infected person.

The HIV virus is very fragile outside the body and is inactivated by exposure to air or bleach solutions. Preventing the spread of HIV infection in the community can be accomplished several different ways such as practicing sexual abstinence, having a long-term monogamous relationship with an uninfected partner, using a latex condom, and by eliminating the sharing or use of unsterilized needles.

Precautions for the emergency responders include the wearing of latex gloves and eye protection when working with injured persons. Disposable CPR masks should be used when performing resuscitation techniques.

Cyber-Cons On The Prowl

by

Nick Lafleur

The time is getting nearer when every one is anticipating the wonders of the New Year. Some people are making their appointments already for the first of the year, others have booked passage on airlines or cruise lines to experience the 1st in multiple time zones. Speculation is rampant about what will happen with the Y2K issue, theories are being tested, contingencies are being planned. If someone you know doesn't have information on the Y2K issue, they at least have an opinion. Truly, it's the latest "buzz".

In the midst of all of the action, there are of course, people who are getting rich. Not in the sense of business owners or consultants working within the realm of the problem, but our not so favorite people, the Cyber-Cons. Did you think you were safe? It was really only a matter of time before these savvy entrepreneurs would take advantage of the latest profit making idea.

The beauty of this venture (to them) is they never have to leave their home, they can use the same tactics they've used for years, there is really no planning necessary, and they can make money the old fashioned way, from someone else. Unlike demographic scams, or focus group cons as it were, where the con artist picks a particular target or a particular topic to focus on, the Y2K issue opens a forum within which everyone can be a target (or mark) quite often, it can even seem legitimate.

Everyone has either heard of or been the victim of a telephone swindle of some sort. Ranging from the wry salesperson that needs some personal info to complete the sale, to a customer that asks the switchboard operator of a business to give them an outside line, thereby accessing the systems long distance network and gaining his/her own personal long distance carrier, at the companies expense.
Perhaps you've heard of the "short change artist", who takes advantage of a busy store clerk, and the "customer is always right" routine to pull a switch at the counter. Working in retail for many years, I've seen people return stolen merchandise for a refund, put more expensive items in less expensive boxes, or simply stuff items down their shirts.

Today however, and in the next several months, the con has changed. Here is the new frontier, however temporarily we must be aware. To make it simple, here is a short list of what to look for.

- Bank reps calling to verify your account, and asking you for the account number.
- Credit card companies calling to make sure your card will work in the new year, and asking you to verify the credit card number.
- Lending institution reps verifying your loan account numbers.
- Foreclosure specialists that say they can stop the foreclosure on your home for a small fee, by acting as a liaison between you and the mortgage company. (for more information go to http://www.americanfinsvcs.org/news and check the news flash section

To sum up, anyone who calls or approaches you, and says they are working for your best interests, but need you to provide personal information, which they should have but don't. That is the clear and present signal of a possible scam. Any legitimate company, banking or otherwise, will have your personal information on hand. If for some reason the mysterious Y2K bug cries havoc and let's loose the proverbial dogs of war, then all personal information should be given in person, at the place that it is needed (bank etc.) In the case of credit card companies, letters should be written, that can be verified, and you should make the calls to those institutions, instead of receiving a call before dinner from some helpful employee of "We're here to help you, Inc." So for the next few months, citizen beware, anything that looks, smells, or acts like a scam, has the high probability of being a scam. Check and double check everything, and never give out personal information over the phone. Technology being a terrific tool in our culture, nothing beats the old paper and pen, or the personal touch of being there yourself.

Leaving Children Home Alone

by

Nick LaFleur

In reference to the age a child can be left at home alone, first, it varies from state to state. Whereas some states don't specify the age within their laws, some have specific definitions of neglect and types thereof. It can also vary from county to county. Most experts agree that a child should be at least 12 years old to be left alone, and 15 to care for younger siblings.

Parents always have a high opinion of their child, but in terms of practical application, and for the child's safety, these questions should be answered, fully, honestly and realistically.
The questions parents must ask themselves are:

Is my child emotionally ready to be left alone? Is the child afraid to be left alone? Get the child's opinion on this. Age has very little to do with maturity and the child should be given the opportunity to address any concerns they may have. Has the child had any training in handling unmanifested events? Does the child know about safety in dealing with visitors? Has there been discussion with the parents in preparation of the child being alone? Is the child able to make informed decisions and use good judgment?

How long will the child be alone? Is it really necessary for the child to be alone? If left alone, will the child have the necessary tools to be safe, both emotionally and physically until the parent's return? Basic necessities such as plenty of food and first-aid supplies should be considered. Food that is pre-cooked will be safer for younger children to prepare, rather than risking preparation via conventional means such as ovens or stovetops. First-aid supplies such as band-aids, topical burn solutions, anti-septic ointments, aspirins or medications the child requires, as well as the knowledge of using such items is paramount.

Are there resources provided for the child in case of emergency? Does the child have training in using 911 and does the child know what information to give authorities? When necessary, writing down all pertinent information can provide the child with the confidence and ability to give out crucial time sensitive information to emergency teams. Even address and phone numbers are hard to remember under times of mental duress. Are there numbers of neighbors or relatives that the child can use if needed?

Are there plans in the home that the child is familiar with in case of an emergency? Does the home have a fire plan, evacuation route etc. Has the family practiced using these plans together as well as individually? Emergency plans are only good when practiced, and should be executed fully to make sure every aspect of the plan works and is practical. Does the child know what to do in case of a home emergency, such as a broken pipe, power outage, water leak, gas leak, electrical malfunction etc?

Finally, what are the state laws regarding leaving children at home?

For the state laws, you must contact the child welfare or protection agencies within a particular county or locale. Never assume that because there no are publicized guidelines specifying these topics, that there are no laws or regulations. In some cases, what we may think of as routine within a particular family structure may in fact be looked upon by certain laws as neglect or even abuse. Researching the law is also a good way to provide anyone with additional advice and assistance when making such crucial decisions. There are a number of local and state agencies that have the resources to answer many important questions. The city directory of most local phone books is a good place to start.

Internet Safety Tips for Children

by

Nick Lafleur

General Tips

- Parental Supervision is the number one tool against child stalkers.

- Child education is next. Talk with your children, become involved without becoming controlling.

- Filtering software and family rules should be added to insure and maintain a safe environment.

- Trust should be built between the child and parents.

- Make children aware of chatting dangers, child predators, and tactics. Sheltering children from such things will not help them. Their ability to identify risks is sometimes all that stands between safety and danger.

- Pornographic sites are rampant, even using search engines will yield such content. Knowing this, establish what is appropriate and what is not appropriate viewing material with your child.

- Child predators are widespread but not everyone is a criminal. Know the indicators, and establish policies with your child about what to do if the perceive a risk. Make them feel strong about not revealing their personal information and about saying NO when they feel threatened in any way.

Chat Tips

- Never give out your real name.

- Never give out your address or phone number.

- Never give out the area you live in within your city.

- Never give out your email to strangers. If you want to make new friends and establish email contact, use an online resource such as HOTMAIL www.hotmail.com which gives you email access on the Internet without compromising your personal information.
- Never discuss your personal life, family life or other sensitive topics such as these. Some people use such topics to get closer to children and build a false sense of trust with them.

- Do not volunteer any personal information as to your daily routine, activities, school/club functions or interests, outside basic conversation.

- Never assume someone’s age, gender, location, name or intent. The “tricks of the trade” of most stalkers include creating an identity that the child will identify with, and it is not uncommon to switch genders and age to get close to the child.

- Use caution if someone is paying special attention to your child and there is an obvious age difference. Not everyone is a criminal, but there are indicators such as age, that you must watch out for.

Internet and Email

- Never download anything from someone you don't know, either via email, or ICQ (www.icq.com) IRC (www.mirc.co.uk), etc.

- Never open any attachments in your email from someone you don't know.

- Never open without virus scanning, attachments from friends, if that attachment was forwarded multiple times.

- Never access web sites that ask your personal information or ask you to start programs within the web site without parental supervision.

Top rated Internet filtering tools. Priced about 40 dollars each.

www.surfwatch.com
www.netnanny.com
www.cyberpatrol.com (good one for AOL)
www.cybersitter.com

The above software gives parents the ability to filter out unwanted content, subject matter, specific pages, topics, and more. Although most settings are manual, there are some automated built in settings as well. Use the links above to find out more.

Internet Browser Built In Protection

Internet Explorer 4x and 5x

- Click HELP.
- Click "CONTENTS and INDEX"
- Click the INDEX tab.
- Type the word FILTER.
- Select "filtering inappropriate content.
- Choose your options.

Netscape Navigator/Communicator 4x

- Click HELP.
- Click NETWATCH
- A web page will open with on screen instructions for setting up NetWatch.

Awareness Conditioning for Personal Safety

by

Nick LaFleur

We all have some concept of what it means to be aware of our surroundings. Whether it be in terms of paying attention at work or taking care on trips not to get lost. In many ways we practice awareness without even realizing it, much the same way we do most instinctive things. Awareness is a natural defensive mechanism inherent in all people. The challenge is in drawing upon this instinct at will instead of relying on pure chance or natural ability.

Times when we had that "feeling" that something wasn't right, or when we performed some physical feat of dexterity that can't easily be repeated, these are times when our awareness was at a natural high and enabled our other senses to perform that much more acutely.

Awareness plays a role important roles in everything from personal success and organization to safety and well being. While we learn to pay attention to certain aspects of our lives in segments, such as learning how to drive, learning to budget money, or learning a particular aspect of a job, we can also hone our awareness skills on a direct level, both conscious and subconscious. We can target specific senses either together or separately and increase their level of acuity thereby increasing our overall awareness levels. Doing so requires very little actual time investment for the training, but a lifelong commitment to continued application for the fine tuning and deliberate active use in daily life.

Conditioning can take the role of self targeted verbal commands, mental visualization, task specific training or generalized focus. We can, for example, practice being more visually aware for a particular sport, or we can spread the training for visual alertness in every day life. We can train our auditory acuteness to increase our effectiveness in a leisure time activity such as composing music, or tune our hearing for a more self defense oriented activity such as when we are in noisy surroundings and need to filter out annoying sounds to ensure our safety from unknown or unforeseen sources.

Training for specific activities or for unknown threats is essentially the same, with focus directed to all our senses being used together, wherein the parts are trained individually for increased skill as a whole. This synergistic approach to awareness training will also increase the amount of pleasure we get from leisure activities, and the amount of safety we get from defense measures. In as little as 7 days we can begin to notice dramatic changes in what we see, hear, taste, feel and smell. Age makes no difference to the training, neither does physical fitness. Individuals with specific handicaps can benefit from awareness training by increasing the level of acuteness in areas where they are weak or by sharpening existing strengths.

Awareness training spans the gamut from children to adults, from sports to self defense, from hobby to full time training commitment. Combing physical aspects with the mental tools sharpened with awareness training, individuals can attain goals that once seemed too great or too advanced. During any activity, care should be given to the training of the senses, to effectively band together the mind, body and spirit into an overall synergistic machine that uses the individual parts to help each other achieve both well being and safety. Missing one part of the mind-body-spirit equation can lead to undesired results and leaves us performing at only a fraction of our total capability.

Chatting Terms and Abbreviations

by

Nick LaFleur

If you are a parent and have ever watched your child chatting, you may have seen some very interesting things. Among them, letters or words that make no sense at all. Below are the best examples of these and their definitions.

AFK: Away from the keyboard.
BBIAB: Be back in a bit
BRB: Be right back.
BBL: Be back later
BTW: By the way.
DCC: Direct Computer Connection. A method of connecting from one IP address to another so that users can chat independently of the chat server they are on. Also used for sending files back and forth on IRC
FAQ: Frequently asked questions.
FLAMING: the bashing or attacking of someone. To get flamed is to get verbally attacked for doing something that the group disapproves of.
FWIW: For what it's worth.
GMTA: Great minds think alike.
IMHO or IMO: In my humble opinion or In my opinion.
IC: I see.
ICQ: I Seek You. An Internet based program that combines chat, email, a contact list, address book, and other features designed to be used as a means for people to get together online. For more information contact www.mirabilis.com or www.icq.com
IK: I know.
IRC: Internet Relay Chat. Currently the most common Internet chatting network. A system of networks from all over the world, accessed by chat programs such as mIRC (www.mirc.co.uk). Users can create channels or rooms where multiple people can type text, communicate via private messages, or send files back and forth. IRC is like the Internet version of the local mall.
IRL: In real life
J/K: Just kidding.
L8R: Later. (As in see you later)
LAMER: Derogatory term for a not so great user.
LMAO: Laughing my (expletive) off. Also seen as RALMAO.
LOL: Laughing out loud.
LTNS: Long time no see.
Nick: Short for Nickname. The alias used in most chat programs in place of a users real name. Nicknames are excellent for providing anonymity, but can also be used by predators to accomplish the same thing
NP: No problem.
RAL: Rolling around laughing.
ROFL: Rolling on the floor laughing.
RTFM: Read the manual. In other words, read the help file before asking questions.

WB: Welcome back.
TIA: Thanks in advance.
TTFN: Ta ta for now.
TTYL: Talk to ya later.
Url: Uniform Resource Locator. The address you enter when surfing.
Such as www.prореresearchgroup.com
Warez: Simply defined, software. Common uses are Shareware (software you can download that expires after a certain period of time if the user does not purchase it) and Freeware (software that is downloaded free of charge). In chat circles warez also refers to the trading of registered programs. Commonly referred to as "pirating".

These are the most common acronyms. Parents who wish to be shown the less tasteful acronyms as a matter of knowing what is being said, may email info@proresearchgroup.com with the subject "Emoticons" for more information.

Fundamentals of Vehicle Safety

by

Wade M. Knapp, CPS

Anyone who drives a vehicle should be aware of the risks associated with such an endeavor. The risks which accompany the operation of a motor vehicle are many; traffic accidents, break-downs, flat tires, vandalism, vehicle theft, and carjacking are just a few of these risks. To reduce the likelihood of these risks occurring we must first be aware of their presence and then take steps to manage these threats. The following are some fundamental safety precautions to consider when operating a motor vehicle.

General Vehicle Safety

- Always keep the vehicle's doors locked, whether inside or out of the vehicle.
- Keep the vehicle's windows rolled up when driving or when the vehicle is parked.
- Consider installing an alarm on the vehicle.
- Consider installing tinted windows on the vehicle which make seeing in the vehicle more difficult.
- Use a locking gas cap.
- Consider installing an automatic garage door opener at your residence.
- Inspect the vehicle daily for signs of tampering or entry.
- Consider obtaining theft insurance for the vehicle.
- Have the vehicle equipped with some form of communications such as a cellular telephone or CB radio.
- A plastic cover can be placed over the license plate to prevent tampering.
- Maintain the vehicle in good working condition.
- Consider installing tires which will run even when flat.
- Don't hide a spare vehicle key any where on the vehicle, keep a spare key in your purse or wallet.
- Keep the vehicle's gas tank at least half full at all times.
- Keep the windshield and all other windows in the vehicle clean.
- Keep a good spare tire in the vehicle and learn how to change your vehicle's tires.
- Only allow the vehicle to be serviced by reputable mechanics and service centers.
- Consider maintaining the following emergency items in the vehicle:
  - A small tool kit.
  - Jumper cables.
  - A flashlight.
  - Local maps.
  - Change for emergency telephone calls.
  - A first-aid kit.
  - A blanket
  - An emergency product which repairs flat tires.
  - A list of emergency telephone numbers for automobile service centers and towing services.

Parking Lot Safety

- Never leave the vehicle unlocked while it is parked.

- Whenever possible, park in secured parking garages.
- When possible , use parking facilities with an attendant or security officer.
- Remember to always be aware of your surroundings while in parking garages. Be observant.
- When using parking garages, avoid secluded areas of the garage and park in a main aisle whenever possible.
- Consider parking on the upper levels of the garage, they are less accessible from the street.
- If the parking garage utilizes security cameras attempt to park in an area where your vehicle will be viewed by these cameras.
- Always remember where you parked your vehicle.
- If you rent a parking space, refrain from placing your name anywhere on the parking space.
- If you must leave keys with a parking attendant, leave only the vehicle's ignition key.
- Avoid parking on the street after nightfall.
- When you have to park during night hours, park in well lighted areas.
- Look around the area before exiting the vehicle.
- Upon exiting the vehicle, move quickly to secure area.
- Have your keys ready before approaching the vehicle.
- Before entering the vehicle, check inside for suspicious items or persons hiding in the vehicle.
- Don't leave purses, luggage, packages, etc. in the passenger compartment of the vehicle. Lock valuable items in the truck while you are away from the vehicle.
- When returning to the vehicle, if you suspect something is wrong or perceive a threat, **Do Not Approach The Vehicle - Leave The Area and Notify The Police.**

Safety While Driving

- Always be aware of your environment while driving.
- Plan your travel routes in advance and vary them often.
- While driving, keep the doors locked.
- Keep windows rolled up and use air-conditioning to control the temperature of the vehicle's passenger compartment
- While driving, keep the vehicle under control.
- Drive defensively.
- Always wear your safety belts and require all passengers to wear safety belts, restrain young children properly in safety seats.
- Refrain from driving at excessive speeds.
- Be cautious and be aware of other traffic when approaching side streets, exit ramps or merging lanes.
- Maintain adequate maneuvering distance between you and other vehicles.
- If a suspicious person approaches or attempts to enter your vehicle, blow the horn and safely drive away.
- Never give strangers a ride.
- If you think someone is following you, don't drive home. Drive to a well lighted area where people are located and notify the police. Give the police a description of the suspicious vehicle.

Biographical Profiling for Personal Safety

by

Wade M. Knapp, CPS

Biographical Profiling is a systematic process in which information regarding an individual's personal history (medical, occupational, family, travel habits, etc.) is collected, recorded and stored in a format which is easily retrievable for use in the event of an emergency involving that individual. The primary reason for creating a biographical profile is to have a complete record of an individual's personal background that can be used by emergency response personnel such as emergency medical services, law enforcement officers, doctors and nurses, etc.

There are several specific situations in which background information is critical to resolving an emergency. The first is an adult or child who has become lost, missing or abducted. U.S. Justice Department annual statistics indicate that approximately 1 million children in the United States become missing, abducted, or are runaways. In addition, it is estimated that over 40,000 adults in the United States become missing annually, and that doesn't include overseas kidnaping. If situations such as these occur, law enforcement officials would require detailed personal information about the child or adult in order to conduct a thorough investigation and / or recover the individual. Biographical information which would be useful to law enforcement officials during an abduction case would include; a complete personal history, medical history, information regarding personal habits, friends and relatives, a set of fingerprints, some form of DNA sample such as blood, hair, or cheek/saliva cells, photos and a videotape of the individual.

Another type of emergency situation which requires detailed biographical information is medical emergencies. Emergency medical situations can arise at anytime. These emergencies can vary from complications arising from an illness or disease, motor vehicle accidents, natural disasters, etc. They can occur with individuals in home healthcare settings, during travel, at work, with students while on field trips or while riding a schools bus, etc. The one thing that any severe medical emergency has in common is that the individual effected will require treatment at a hospital. Hospital personnel in the Emergency Department will generally require your medical history in order to treat you effectively. This means that you or a family member will have to relate this information to hospital personnel. In addition to treatment in a hospital, what about emergency medical service (EMS) personnel that arrive at the initial location of the emergency. These EMS responders must begin emergency treatment and stabilize the patient for transport to the hospital. They also require information regarding your medical history in order to render proper care.

A good medical information history should include information regarding your doctor, specific medications taken, special treatments, equipment needs, special diets, allergies, medical insurance information, or any other information critical to your treatment. This information should be prepared in advance (and updated regularly) and stored until needed for such an emergency.

To illustrate the problem created by not having personal medical information available, consider a problem that was encountered during the 1999 Hurricane Floyd evacuation. During this evacuation, it was noted that the vast majority of patients from home healthcare situations reported to emergency shelters without bringing their medical information with them. This created a situation in which medical personnel staffing the shelter didn't have the information needed to properly care for the evacuees. This situation was echoed throughout the entire eastern coast.

The final situation I will cover in which biographical information can be useful is traveling. This includes both domestic and overseas travel. The two major threats associated with traveling, that would require personal background information, are kidnaping and medical emergencies. These risks effect anyone who travels either for business or leisure. Medical emergencies which occur during travel would require fundamentally the same information mentioned earlier in this article, however it should be remembered that while traveling, you are away from your home and quick access to your personal information. This means that your personal medical history will not be available to emergency medical personnel providing treatment, unless you are able to verbally relate this information to them or have a family member present that can supply the information. Preparing this information in advance and carrying it with you while traveling would save valuable time in the event you suffer an injury or illness requiring treatment.

Another situation which could benefit from biographical information is Executive Protection. Security personnel engaged in the Executive Protection services should be extremely concerned with having personal background information regarding their client while traveling. However, even the average tourist can become the target of a political or ransom motivated kidnaping. In a situation such as this, law enforcement agencies would require extensive personal background on the individual kidnaped. This means that the individual’s family would be responsible for gathering this information and making it available to law enforcement. In the case of Executive Protection, it would be the responsibility of the Detail Leader of the protection team to gather and make this information available. The information that would generally be required will reflect the categories listed above when I mentioned missing or abducted persons. Security personnel would also be confronted by the risk of a possible medical emergency involving a client and should take steps to insure that an adequate medical history of their client is available.

In conclusion, I would like to emphasize that this article has illustrate only a few of the many situations in which biographical information would be useful during an emergency. Biographical profiling is a tool which can be utilized to enhance anyone’s personal safety. It is one part of an overall personal safety plan. The process of creating such records may be slightly laborious, however, if a time comes when this type of information is needed, the time spent preparing it will pay for itself many times over.

Copyright Bibliography

Fundamental Concepts of Terrorism, by Wade M. Knapp, CPS Copyright ©1999

Characteristics of Biological Warfare Agents, by Lee A. Knapp, RN, CEN Copyright ©1999

Understanding the Toxic Effects of Chemical Warfare Agents, by Lee A. Knapp, RN, CEN Copyright ©1999

Fundamentals of Encryption, by Nick LaFleur Copyright ©1999

Computer Viruses and Solutions, by Nick LaFleur Copyright ©2000

Understanding the Impact of Biological & Chemical Terrorism, by Wade M. Knapp, CPS Copyright ©2000

Using Passwords in a Computing Environment, by Nick LaFleur Copyright ©1999

Telephoned Bomb Threat Procedures, by Wade M. Knapp, CPS Copyright ©1999

Recognizing Letter and Package Bombs, by Wade M. Knapp, CPS Copyright ©1999

Understanding Crime Risk Management, by Wade M. Knapp, CPS Copyright ©2000

Security Patrol Operations, by Wade M. Knapp, CPS Copyright ©1999

Security Patrol Vehicle Maintenance, by Nick LaFleur Copyright ©1999

Safety at Automated Bank Teller Machines (ATM's), by Wade M. Knapp, CPS Copyright ©1998

Safety Precautions While Staying at Hotels or Motels, by Wade M. Knapp, CPS Copyright ©1998

Protection Officers and the Press, by Wade M. Knapp, CPS Copyright ©2000

First Aid Basics, by Lee A. Knapp, RN, CEN Copyright ©1999

Cyber-Cons On The Prowl, by Nick LaFleur Copyright ©1999

Leaving Children Home Alone, by Nick LaFleur Copyright ©1999

Internet Safety Tips for Children, by Nick LaFleur Copyright ©1999

Awareness Conditioning for Personal Safety, by Nick LaFleur Copyright ©1999

Chatting Terms and Abbreviations, by Nick LaFleur Copyright ©1999

Fundamentals of Vehicle Safety, by Wade M. Knapp, CPS Copyright ©1998

Biographical Profiling for Personal Safety, by Wade M. Knapp, CPS Copyright ©2000

About the Authors

Wade M. Knapp, CPS

Mr. Knapp is President of Protective Research Group, a protection & safety consulting firm located in Jacksonville, Florida. He is a Certified Protection Specialist with over 22 years experience in the protection industry, including 10 years in security management. He is a graduate of Executive Security International, Aspen CO., and has obtained education in Law Enforcement, Security Management, Biological & Chemical Terrorism, Disaster Management, Advanced Hazmat Life Support, and Self-Defense. In addition to his career in Security Management, he is also an experienced Bodyguard, Licensed Security Instructor, Safety & Security Lecturer, Safety & Security author, a former Private Investigator, and a 1st Degree Black Belt and Self-Defense Instructor.

Lee A. Knapp, RN, CEN

Mrs. Knapp is Vice-President of Protective Research Group, a protection & safety consulting firm located in Jacksonville, Florida. She is a Registered Nurse and Certified Emergency Nurse with over 16 years experience in the medical industry, including over 14 years in the field of emergency nursing. Mrs. Knapp is a graduate of Marshall University School of Nursing, and has an extensive background in the field of emergency medicine. Certifications and education include: Basic Life Support (BLS), Basic Life Support Instructor, Advanced Cardiac Life Support (ACLS), Advanced Hazmat Life Support (AHLS), Advanced Hazmat Life Support Instructor, Biological & Chemical Terrorism, and nursing management. In addition, she is an experienced Medical & Safety Lecturer, and NBC Terrorism training coordinator for the Emergency Department Staff at St. Vincent's Medical Center in Jacksonville, Florida.

Nick LaFleur

Mr. Lafleur is Vice-President of Protective Research Group, a protection & safety consulting firm located in Jacksonville, Florida. He has over 10 years experience in the protection industry, including 6 years in security management. He has extensive expertise in the fields of Computer & Information Security, Investigative Technologies, and Physical Security Planning. He is a Licensed Private Investigator, Self Defense Instructor, and Safety & Security Author and Lecturer

For information about Protective Research Group contact:

Protective Research Group
1740 Manning St.
Jacksonville, Florida 32207
Telephone: 904.285.8520
On the Web: www.proresearchgroup.com
Email: info@proresearchgroup.com